

109
COMPLETED

✓ 4.674/7:C83
**COUNTERINTELLIGENCE AND NATIONAL
SECURITY INFORMATION**

ORIGINAL
MK 110
HEARING

BEFORE A

SUBCOMMITTEE OF THE

COMMITTEE ON

GOVERNMENT OPERATIONS

HOUSE OF REPRESENTATIVES

NINETY-NINTH CONGRESS

FIRST SESSION

JUNE 17, 1985

Printed for the use of the Committee on Government Operations



U.S. GOVERNMENT PRINTING OFFICE

WASHINGTON : 1986

55-822 O

BEST COPY AVAILABLE

COMMITTEE ON GOVERNMENT OPERATIONS

JACK BROOKS, Texas, *Chairman*

DON FUQUA, Florida
JOHN CONYERS, Jr., Michigan
CARDISS COLLINS, Illinois
GLENN ENGLISH, Oklahoma
HENRY A. WAXMAN, California
TED WEISS, New York
MIKE SYNAR, Oklahoma
STEPHEN L. NEAL, North Carolina
DOUG BARNARD, Jr., Georgia
BARNEY FRANK, Massachusetts
TOM LANTOS, California
ROBERT E. WISE, Jr., West Virginia
BARBARA BOXER, California
SANDER M. LEVIN, Michigan
MAJOR R. OWENS, New York
EDOLPHUS TOWNS, New York
JOHN M. SPRATT, Jr., South Carolina
JOE KOLTER, Pennsylvania
BEN ERDREICH, Alabama
GERALD D. KLECZKA, Wisconsin
ALBERT G. BUSTAMANTE, Texas
MATTHEW G. MARTINEZ, California

FRANK HORTON, New York
THOMAS N. KINDNESS, Ohio
ROBERT S. WALKER, Pennsylvania
WILLIAM F. CLINGER, Jr., Pennsylvania
ALFRED A. (AL) McCANDLESS, California
LARRY E. CRAIG, Idaho
HOWARD C. NEILSON, Utah
JIM SAXTON, New Jersey
PATRICK L. SWINDALL, Georgia
THOMAS D. (TOM) DELAY, Texas
DAVID S. MONSON, Utah
JOSEPH J. DIOGUARDI, New York
JOHN G. ROWLAND, Connecticut
RICHARD K. ARMEY, Texas
JIM LIGHTFOOT, Iowa
JOHN R. MILLER, Washington

WILLIAM M. JONES, *General Counsel*

JOHN E. MOORE, *Staff Administrator*

STEPHEN M. DANIELS, *Minority Staff Director and Counsel*

GOVERNMENT INFORMATION, JUSTICE, AND AGRICULTURE SUBCOMMITTEE

GLENN ENGLISH, Oklahoma, *Chairman*

GERALD D. KLECZKA, Wisconsin
STEPHEN L. NEAL, North Carolina
ROBERT E. WISE, Jr., West Virginia
EDOLPHUS TOWNS, New York
JOHN M. SPRATT, Jr., South Carolina

THOMAS N. KINDNESS, Ohio
JIM LIGHTFOOT, Iowa
JOSEPH J. DIOGUARDI, New York
JOHN R. MILLER, Washington

EX OFFICIO

JACK BROOKS, Texas

FRANK HORTON, New York

WILLIAM G. LAWRENCE, *Counsel*

EUPHON L. METZGER, *Clerk*

JOHN J. PARISI, *Minority Professional Staff*

(11)

BEST COPY AVAILABLE

CONTENTS

	Page
Hearing held on June 17, 1985.....	1
Statement of:	
Allen, Robert C., Director, Security Policy, Office of Chief of Naval Operations, U.S. Navy.....	92
English, Hon. Glenn, a Representative in Congress from the State of Oklahoma, and chairman, Government Information, Justice, and Agriculture Subcommittee: Opening statement.....	1
McCullah, Lanny E., Assistant Director for Counterintelligence, Naval Investigative Service, U.S. Navy.....	63
Parker, Philip A., Deputy Assistant Director, Intelligence Division, Federal Bureau of Investigation, accompanied by Harry Porter, special agent.....	27
Snider, L. Britt, Director, Office of Counterintelligence and Security Policy, Department of Defense, accompanied by Jack Donnelly, Director, Counterintelligence and Investigative Programs, and Maynard Anderson, Director, Security Plans and Programs.....	42
Thurman, Bill W., Deputy Director, National Security and International Affairs Division, General Accounting Office, accompanied by James Reid and Irving Boker, staff members.....	4
Letters, statements, etc., submitted for the record by:	
Allen, Robert C., Director, Security Policy, Office of Chief of Naval Operations, U.S. Navy: Prepared statement.....	94-101
McCullah, Lanny E., Assistant Director for Counterintelligence, Naval Investigative Service, U.S. Navy: Prepared statement.....	66-91
Miller, Hon. John R., a Representative in Congress from the State of Washington: Prepared statement.....	3
Snider, L. Britt, Director, Office of Counterintelligence and Security Policy, Department of Defense: Prepared statement.....	44-55
Thurman, Bill W., Deputy Director, National Security and International Affairs Division, General Accounting Office: Prepared statement.....	9-16

(iii)

BEST COPY AVAILABLE

COUNTERINTELLIGENCE AND NATIONAL SECURITY INFORMATION

MONDAY, JUNE 17, 1985

HOUSE OF REPRESENTATIVES,
GOVERNMENT INFORMATION, JUSTICE,
AND AGRICULTURE SUBCOMMITTEE
OF THE COMMITTEE ON GOVERNMENT OPERATIONS,
Washington, DC.

The subcommittee met, pursuant to notice, at 1:30 p.m., in room 2247, Rayburn House Office Building, Hon. Glenn English (chairman of the subcommittee) presiding.

Present: Representatives Glenn English, Stephen L. Neal, John M. Spratt, Jr., Jim Lightfoot, and John R. Miller.

Also present: William G. Lawrence, counsel; Euphon Metzger, clerk; and John J. Parisi, minority professional staff, Committee on Government Operations.

OPENING STATEMENT OF CHAIRMAN ENGLISH

Mr. ENGLISH. The hearing will come to order.

In a country that has become almost numbed by daily reports of violent crime, espionage cases still chill our blood. While most other crimes may seem unrelated to us as individuals, each espionage case bleeds our entire Nation of its ability to defend us against hostile enemies.

We do not meet this afternoon to delve into the circumstances of any particular case, but rather to begin a process of determining the size of the problem and measuring the ability of our Government to fight it. And it is a tough fight.

This is a free Nation, not a police state. Our citizens are presumed to be trustworthy and patriotic. Our processes of government are open, and information circulates freely.

But our freedoms generate responsibilities which some citizens are unwilling to honor. The FBI reports that almost all the instances of espionage that they have detected in the past two decades involve Americans who have volunteered secret information to our enemies, not persons which have been carefully recruited. Their motivation was greed, or revenge, or a thirst for excitement.

In our hearings we will be asking: What is the Government's response to the threat of espionage, and what more needs to be done? We have some pretty good insights already.

We are told that there are more than 4 million persons already holding security clearances, with thousands of requests for new clearances every month. Between new investigations and periodic

(1)

BEST COPY AVAILABLE

reinvestigations of people cleared in years past, our ability to do a prompt and thorough job has diminished.

The Defense Investigative Service has established a quota of 40,000 reinvestigations of top secret clearance holders per year, but there are 725,000 of them. Rather than being reinvestigated every 5 years, as the regulations require, these numbers work out to every 17 years instead.

Demands on the Defense Investigative Service became so great that in 1980 it was forced to declare a 2-year moratorium on reinvestigations of clearance holders just to try to reduce its backlog of requests of new investigations.

I have recently been informed of a situation which, as ridiculous as it sounds, might be contributing to this workload. A man who works as a consultant to Department of Defense contractors came into the subcommittee offices. He told us that he works alone, but is incorporated for business reasons. Because State law requires at least two persons to incorporate, he named his wife as a member of his board of directors, not an uncommon practice in the world of small business.

He has just been informed that his wife is being investigated for a secret clearance because she is on his corporate board. This woman is a kindergarten teacher. She never sees or has access to any classified information. She does no work of any kind for her husband's firm. All classified information that her husband consults on is maintained at the offices of the Department of Defense contractor, never in his home.

How many more of these cases are there?

The amount of information considered to require classification has also increased, and will probably continue to grow. President Reagan recently issued new classification rules which broadened classification categories and watered down the requirements for what can be classified.

The proliferation of classified information and the numbers of persons with clearances can have unhealthy effects, and rather than improving security, can actually damage it as the whole classification process becomes cheapened.

I believe that there could be a significant reduction in the numbers of people with clearances. We could start with people, including kindergarten teachers, and firms holding current clearances that haven't had access to secret documents for a period of time.

This would also free up investigators to work on the more urgent cases in which violations are occurring in extremely sensitive, highly secured areas and by people who are necessarily cleared, as in the Walker case.

But that is only part of the problem. In addition to the record numbers of people holding clearances, and the record amount of information now being classified, there is also a record number of Soviet and Eastern bloc "diplomats" and trade representatives in this country. The totals may exceed 4,000, with the FBI estimating that perhaps 40 percent of them are devoted to spying.

This has created monumental problems for the Bureau in simply keeping track of them. While this Nation embraces free trade and free travel, I have to wonder if we haven't been generous to a fault in this area, and whether we shouldn't admit the same number of

Soviets into the United States as the number of Americans that they admit to Russia. We should also think about exercising some of the same travel limits on the Soviets that they impose on us.

There are considerations involved in espionage cases which transcend the usual criminal case. For example, it is essential to know not only a person's guilt, but also what information was passed to the hostile power, and who their contacts were, so that appropriate damage control actions can be promptly taken.

We will be asking whether our statutes are sufficient for the FBI and our courts to do their jobs, whether changing circumstances might justify additions to our criminal code or rules of procedure.

Since espionage has become a mercenary activity in some people's minds, we should make sure that the price they pay when caught far exceeds the few thousand dollars they might stand to gain by selling out their country.

As I told our witnesses in their letters of invitation, we will be holding additional hearings, some in executive session. This is an open hearing, and any question which will require a classified answer should be identified as such, and reserved for a future closed hearing.

Without objection, the prepared statement from Mr. Miller will be inserted at this point.

[The prepared statement of Mr. Miller follows:]

PREPARED STATEMENT OF HON. JOHN R. MILLER

Mr. Chairman, thank you for calling this very timely and important hearing today to examine the effectiveness of our counterintelligence programs. I am especially concerned with this issue in view of the number of sensitive military installations located within my district in Washington State.

Unfortunately, we are all too often moved to action after a tragic event, such as the recent revelations of alleged espionage activities by the Walker family. Recent reports indicate that the Navy and the Pentagon have decided to significantly reduce the number of existing security clearances and the amount of classified documents in an effort to prevent future security leaks.

However, I am concerned that serious efforts to improve our classification system may never come to pass. Over the year, the committee has consistently expressed its deep concern with the overclassification of information, and has recommended action to address this situation. Nevertheless, the consistent pattern of overclassification by the executive branch continues.

Beyond this concern, we must also consider the effectiveness of the different agencies involved in the protection of classified information and the counterespionage efforts by the intelligence community. Finally, other deterrence methods should be reviewed, such as a harsher penalty for those who commit espionage and the increased use of lie detectors in background investigations.

Mr. Chairman, I strongly urge the executive branch to take serious action to prevent future breaches of our security. I look forward to today's hearing and I hope it will serve as a useful discussion of possible options in this regard.

Mr. ENGLISH. We have as our first witness today, Mr. Bill Thurman, who is the Deputy Director of the National Security and International Affairs Division of the General Accounting Office.

Mr. Thurman, please come forward to the table and identify those people who might accompany you.

STATEMENT OF BILL W. THURMAN, DEPUTY DIRECTOR, NATIONAL SECURITY AND INTERNATIONAL AFFAIRS DIVISION, GENERAL ACCOUNTING OFFICE, ACCOMPANIED BY JAMES REID AND IRVING BOKER, STAFF MEMBERS

Mr. THURMAN. Good afternoon, Mr. Chairman.

Accompanying me this afternoon are two people who have worked in this area for a number of years. To my immediate left is Mr. Irving Boker, and to my right Mr. James Reid. Both of these gentlemen are on the staff of our division and have spent a number of years working in the area of security and security protection.

The three of us appreciate the opportunity to appear before you this afternoon to discuss some of the observations we have made on the Government's program for protecting national security.

With your permission, Mr. Chairman, I will try to, in the interest of time, abbreviate my complete statement and perhaps allow additional time for questioning. I understand that you are pressed for time.

Mr. ENGLISH. Mr. Thurman, without objection, your full and complete statement will be made part of the record, so feel free to summarize.

I might say at this point as far as any of our witnesses are concerned, if they care to summarize their testimony, their full, complete written testimony will be made part of the record.

Mr. THURMAN. Thank you, sir.

In recent years, the volume of classified information and the number of people with security clearances to see that information has rapidly increased. The following statistics, which exclude the Central Intelligence Agency and the National Security Agency, give some indication of the dimensions of the problems that the Nation faces in maintaining security for classified information and for effective management of the entire area.

Data that we gathered during 1984 showed that at the end of calendar year 1983, approximately 2.7 million Government employees, including military personnel, had security clearances. This was an increase of about 7½ percent over 1982.

In addition to those numbers, about 1.5 million contractor employees had security clearances, which means that about 4.2 million individuals had clearances at the end of calendar year 1983. At that time, the Department of Defense accounted for 94 percent of the Government employees with clearances and 87 percent of the contractor employees with clearances.

The Department of Defense has advised us recently that as of March 1985, about 2.9 million Department of Defense civilian and military personnel had security clearances and about 1.4 million Department of Defense contractor employees had clearances. This represents an increase over the calendar year 1983 figures for the Department of Defense of about 11 percent.

Over 50 Government agencies, which, of course, include several thousand installations and offices throughout the country and the world, are authorized to handle classified information and are responsible for safeguarding it. According to the Information Security Oversight Office, these agencies, excluding the National Security Agency, generated over 19.5 million classified documents in calen-

BEST COPY AVAILABLE

dar year 1984. This included about 16.6 million for the Department of Defense, or about 85 percent of the total. In addition, there are about 14,000 cleared industrial facilities authorized to handle classified documents.

Executive Order 10450, which was issued in 1953, continues to be the basic authority for the Federal Government's personnel security clearance program. The type of security clearance an individual needs is determined by the classification level of the information to which the individual will have access. Most Government employees with a clearance have a secret which is granted clearance if a national agency check and inquiries produce no serious derogatory information.

The national agency check portion consists of searching the records of certain Federal agencies, such as OPM and the Departments of Justice and State, to determine the existence of any previous investigation or criminal record and to verify citizenship and any military service. The inquiries portion involves sending written inquiries covering specific areas of the subject's background during the past 5 years or since the individual's 18th birthday, whichever is shorter.

A top secret clearance requires the same information but, in addition, it requires a favorable background investigation which covers the same period. The background investigation includes personal interviews with people who know the individual being investigated and a verification of his or her birth date, education, and employment.

In addition to the regular security clearance, the intelligence agencies require that a more extensive or special background investigation be conducted before an individual is granted access to intelligence information, methods, or sources. Such information is referred to as sensitive, compartmented information—so-called SCI. The minimum standards for the special background investigation in this area are prescribed by the Director of Central Intelligence.

The Department of Defense, through the Defense Investigative Service, performs the majority of the personnel investigations conducted by the Federal Government each year. During calendar year 1984, the Defense Investigative Service performed a million investigations involving Department of Defense and industry personnel.

Over the past 10 years, we in GAO have examined various aspects of the Government's program for protecting national security information. I might mention, Mr. Chairman, that attached to my statement is a complete listing of GAO reports issued in this subject area that goes back over 10 years to about 1974, and we would be more than pleased to provide copies of those reports to the subcommittee.

Mr. ENGLISH. It is my understanding, according to counsel, we do have copies of those reports on hand, so thank you very much for the offer.

Mr. THURMAN. In view of the current concerns that are surfacing so dramatically today about the effectiveness of the Nation's systems for protecting classified information, we felt that the results of our work in certain areas might be of particular interest to you and I would like to briefly summarize our observations in these

areas. The first area is that of periodic reinvestigations and the monitoring of cleared employees; the second deals with control of the number of requests for security clearances; and the third deals with the subject of classification guidance and training, and the oversight involved in the classification process itself.

With regard to the first area, the granting of security clearances to Government or contractor employees is only the first step in the protection of national security information. Previously cleared individuals should be periodically reinvestigated and continuously monitored to ensure that their access to classified information remains in the best interests of national security.

As you mentioned, sir, in your opening statement, we found and have noted in our work, as you did, that in June 1981, the Department of Defense placed a moratorium, on periodic reinvestigations for individuals with SCI access because of the investigative backlog resulting from an increased number of initial investigations.

In June 1983, because of improvements in the backlog, and in the turnaround time, the Department of Defense resumed periodic reinvestigations for persons with SCI access, expanded the scope of its periodic reinvestigations of individuals with top secret clearances, and included military personnel. Previously, military personnel with top secret clearances would be reinvestigated only if they were: (1) Given access to SCI, (2) assigned to certain special access programs, or (3) the subject of some derogatory information.

To ensure that the periodic reinvestigations would not adversely impact the overall backlog and case completion time for all investigations, the Department of Defense established an annual quota of 40,000 periodic reinvestigations. With over 100,000 individuals with SCI access and about 500,000 other individuals with top secret clearances in the Department of Defense and industry, it may be several years before the Department can get the reinvestigative process back on schedule considering its already heavy workload for new investigations. We understand that the Department of Defense has recently begun an evaluation of the usefulness of its reinvestigation program. We believe that this is a worthwhile effort and that it may enable the Department of Defense to identify areas where greater emphasis should be placed.

The continuous monitoring of employees who have security clearances is also important. Government agencies and contractors need to pay close attention to employees with emotional, alcohol or drug related or severe financial problems. The Department of Defense requires its contractors to report any adverse information about an employee with a security clearance. During fiscal year 1984, the Defense Industrial Security Clearance Office received 2,400 reports with adverse information and, based on these reports, suspended 24 clearances on an interim basis until the adverse information could be resolved.

The Department of Defense regulations covering military and civilian personnel require the immediate reporting of adverse information, by the most expeditious means possible, to the commander or security officer of the organization to which the subject individual is assigned.

We found, generally, that when derogatory information on an individual is reported, agencies are reluctant to revoke security clear-

ances because such revocation might be considered an adverse action. Agencies prefer to reassign the employee to a position that does not require a clearance to carry out his or her duties.

The second area that I would like to summarize deals with the number of security clearances. While we in the General Accounting Office have not performed any overall evaluation of the need for the number of security clearances that have been issued, our work has indicated that there is a need for greater control over requests for such clearances.

In our February 1983 report, focused only on Department of Defense special access contracts, we recommended that instructions be issued which would require Defense's advance approval of a contractor's nominee for a special background investigation. We also recommended that the Defense Investigative Service return to contractors any requests not containing such an advance approval. The Department did take steps to implement those recommendations.

Department of Defense officials have told us of cases where contractors' employees had security clearances that were in excess of the number needed to perform on classified contracts. Over the years, audit reports by the military services have identified situations where an excess number of security clearances were being requested for military personnel. The Department recognizes this problem and has considered a number of options to try and control the proliferation of security clearances.

Last week, some steps were taken in this regard. On June 10, 1985, the Defense Investigative Service announced a clearance reduction program within industry. The program is designed to identify and eliminate existing security clearances that are no longer required and to tighten up on the procedures used by contractors to request clearances.

The Secretary of Defense has ordered an immediate 10 percent reduction in the number of security clearances held by military and civilian personnel.

The last area I would like to cover, Mr. Chairman, is a brief discussion of the classification of material. There is a connection. The large number of security clearances is driven by the volume of classified material that we have in the Government today. In a report that we issued in March 1981, we identified instances where because of deficiencies in guidance, training, and inspections, some national security information had been improperly classified by contractors—both overclassified and underclassified—and had not been properly managed to protect it.

In the course of this work, we reviewed 235 classified documents to determine if various portions of the documents were classified correctly. Of the 235, 119 or about 51 percent, contained one or more examples of improper classification. Of the 119 documents, 109 had portions that were overclassified and the other 10 had portions that were both underclassified and overclassified.

We found that classification guidance furnished by the Department of Defense was outdated, vague, and inconsistent. We recommended that the Department improve the classification guidance given to contractors, expand the training of contractor employees, and include classification management in its periodic security in-

spection of contractors. The Department of Defense agreed that more training was needed, but noted that a lack of funding and personnel precluded any significant expansion of its training activities in this area.

Mr. Chairman, I am afraid that is not too brief a synopsis of my complete statement, but I think that pretty well summarizes it. We would be pleased to try to respond to any questions you might have.

[The prepared statement of Mr. Thurman follows:]

U.S. GENERAL ACCOUNTING OFFICE

WASHINGTON, D.C.

FOR RELEASE ON DELIVERY
Expected at 1:30 p.m.
Monday, June 17, 1985

STATEMENT OF

BILL W. THURMAN

DEPUTY DIRECTOR

NATIONAL SECURITY AND INTERNATIONAL AFFAIRS DIVISION

BEFORE THE

SUBCOMMITTEE ON GOVERNMENT INFORMATION, JUSTICE AND AGRICULTURE
HOUSE COMMITTEE ON GOVERNMENT INFORMATION

ON

THE GOVERNMENT'S PROGRAM FOR
PROTECTING NATIONAL SECURITY INFORMATION

BEST COPY AVAILABLE

Mr. Chairman and Members of the Subcommittee:

I appreciate the opportunity to appear before you this afternoon to discuss some of the observations we have made on the government's program for protecting national security information.

With me this afternoon are Irv Boker and Jim Reid, who work in the security area.

National security information includes classified information pertaining to national defense and foreign relations. The protection of classified information generally falls into three broad categories--information security, physical security, and personnel security. Briefly, information security involves the proper classification and marking of national security information; physical security involves the safe transmission and secure use and storage of the classified information; and personnel security involves the investigation and adjudication of information concerning an individual, needed to determine that the individual is trustworthy and can be given access to classified information.

The volume of classified information and of people with security clearances to see that information has increased significantly in recent years. The following statistics, which exclude the Central Intelligence Agency and the National Security Agency, give some indications of the dimensions of the problem of maintaining security for classified information and for effective management in the area.

Data that we gathered in 1984 showed that at the end of calendar year 1983, approximately 2.7 million government employees (including the military) had security clearances. This was an increase of about 7.5 percent over 1982. In addition, about 1.5 million contractor employees had security clearances which means that about 4.2 million individuals had security clearances at the end of 1983. At that time, DOD accounted for 94 percent of the government employees and 87 percent of the contractor employees with security clearances.

DOD has advised us that, as of March 1985 about 2.9 million DOD civilian and military personnel had security clearances and about 1.4 million DOD contractor employees had clearances, an increase from December 1983 of almost 11 percent for DOD.

Over 50 government agencies (including several thousand installations and offices) are authorized to handle classified information and are responsible for safeguarding it. According to the Information Security Oversight Office, these agencies, excluding the National Security Agency, generated over 19.5 million classified documents in calendar year 1984 including about 16.6 million for DOD (almost 85 percent of the total). In

BEST COPY AVAILABLE

addition, there are about 14,000 cleared industrial facilities authorized to handle classified documents. The number of classified documents generated by them in calendar year 1984 is unknown; however, they have an inventory of about 16 million classified documents.

Executive orders have governed the classification of national security information since 1940. The current executive order 12356, issued in April 1982, like several orders before it, prescribes three levels of classification--top secret, secret, and confidential--depending on the level of sensitivity of the information and the potential damage that would result from its disclosure.

Executive Order 10450, issued April 27, 1953, is the basic authority for the federal government's personnel security clearance program. The order makes the Office of Personnel Management (OPM) responsible for conducting all competitive service investigations used in determining the suitability of individuals for civilian government employment and as a basis for ensuring that the employment of the individual is clearly consistent with the interests of national security. Some agencies, such as the Departments of Defense, State, and Treasury, are authorized by law, or agreement with OPM, to conduct investigations of competitive service positions.

The type of security clearance an individual needs is determined by the classification level of the information to which the individual will have access. Most government employees with a security clearance have either a secret or top secret clearance. A secret clearance can be granted if a National Agency Check and Inquiries produces no serious derogatory information. The National Agency Check portion consists of searching the records of certain federal agencies such as the OPM and the Departments of Defense, Justice, and State to determine the existence of any previous investigations or a criminal record and to verify citizenship and any military service. The inquiries portion involves sending written inquiries covering specific areas of the subject's background during the past 5 years or since the individual's 18th birthday, whichever is shorter. A top secret clearance requires the same information but, in addition, it requires a favorable background investigation which covers the same period. The background investigation includes personal interviews with people who know the individual being investigated and a verification of his or her birthdate, education, and employment.

In addition to a regular security clearance, the intelligence agencies, including some components of DOD, require that a more extensive, or special background investigation be conducted before an individual is granted access to intelligence information, methods, or sources. Such information is referred to as sensitive compartmented information (SCI). The minimum standards for the special background investigation are prescribed by the Director of Central Intelligence.

DOD, through the Defense Investigative Service, performs the majority of the personnel investigations made each year. These investigations are needed because of new employee hiring, changes in jobs, and retirements; military enlistments, promotions and discharges; new programs; and periodic reinvestigations. During calendar year 1984, the Investigative Service performed 1,071,000 investigations involving DOD and industry personnel.

Over the past 10 years, we have examined various aspects of the government's program for protecting national security information. A listing of pertinent GAO reports is included as an attachment to my statement. We would be pleased to provide copies of any or all of these reports to the Subcommittee.

In view of the current concerns about the effectiveness of the nation's system for protecting classified information, the results of our work in certain areas might be of particular interest to the subcommittee, and I would like to briefly summarize our observations in the following three areas:

- Periodic reinvestigations and continuous monitoring of cleared employees,
- Control of the number of requests for security clearances, and
- Improved classification guidance for contractors.

Need for Periodic Reinvestigations and
Continuous Monitoring of Cleared Employees

The granting of security clearances to government or contractor employees is only the first step in the protection of national security information. Previously cleared individuals should be periodically reinvestigated and continuously monitored to ensure that their access to classified information remains in the best interest of national security. Policies and procedures for such monitoring differ among agencies.

The Federal Personnel Manual, issued by OPM, which applies only to government civilian employees, requires a reinvestigation every 5 years after an individual is placed in a position designated "special sensitive" or "critical sensitive." (These terms are equivalent to an SCI access and top secret clearance, respectively.)

In June 1981, DOD placed a moratorium on periodic reinvestigations for individuals with SCI access because of the investigative backlog resulting from an increased number of initial investigations. In April 1983, because of improvements in the backlog and turnaround time, DOD resumed periodic reinvestigations for persons with SCI access and expanded the scope of its periodic reinvestigations of individuals with top secret

clearances. Included with the individuals with top secret clearances to be reinvestigated were military personnel. Previously, military personnel with top secret clearances would be reinvestigated only if they were (1) given access to SCI, (2) assigned to certain special programs, or (3) the subject of some derogatory information. In those cases involving derogatory information, the investigation was to be limited to that necessary to verify or discount the information.

To ensure that the periodic reinvestigations would not adversely impact the overall backlog and case-completion time for all investigations, DOD established an annual quota of 40,000 periodic reinvestigations. With over 100,000 individuals with SCI access and about 500,000 other individuals with top secret clearances in DOD and industry, it may be several years before DOD can get the reinvestigation process back on schedule, considering its heavy work load of requests for new investigations.

We understand that DOD has recently begun an evaluation of the usefulness of its reinvestigation program. We believe that this is a worthwhile effort and it may enable DOD to identify areas where greater emphasis should be placed. Reinvestigations are currently required only for those individuals who have top secret clearances or SCI access. Over 3.3 million (2,385,000 government and 972,000 contractor) individuals have secret clearances and are not subject to a periodic reinvestigation.

The continuous monitoring of employees who have security clearances is also important. Government agencies and contractors need to pay close attention to employees with emotional, alcohol- or drug-related, or severe financial problems.

DOD requires its contractors, operating some 14,000 cleared facilities that may have access to classified information, to report any adverse information about an employee with a security clearance. This is a formalized reporting process, with the reports being sent to the Defense Industrial Security Clearance Office, which is the central adjudication facility for contractor employees. During fiscal year 1984, the Clearance Office received 2,400 reports with adverse information and, based on these reports, suspended 24 clearances, on an interim basis, until the adverse information could be resolved.

DOD regulations covering military and civilian personnel require the immediate reporting of adverse information, by the most expeditious means possible, to the commander or security officer of the organization to which the subject individual is assigned.

We have found that, when derogatory information on a individual is reported, agencies are reluctant to revoke security clearances because such revocation might be considered an adverse action. Agencies prefer to reassign the employee to a position that does not require a clearance.

Need to Control the Number of Requests
for Security Clearance Investigations

We have not performed any overall evaluation of the need for the number of security clearances that have been issued, however, our work as well as that of DOD internal audit agencies, has indicated there is a need for greater control over requests for security clearances. In our February 1983 report, which pertained only to DOD special access contracts, we recommended that instructions be issued that would require DOD's advance approval of a contractor's nominee for a special background investigation. We also recommended that the Defense Investigative Service return to contractors any requests not containing the advance approval. DOD took steps to implement our recommendations.

Some contractors said that it was possible to circumvent the system and that they were submitting more requests than they needed. Two contractors, who acknowledged requesting a few more special access authorizations than they needed, said that delays by DOD in completing investigations forced them into an untenable situation. If they received a new contract or needed additional employees for an existing contract, they could transfer appropriately cleared employees from other contracts (which would delay that work), hire other contractors' employees who already had special access authorizations (which was costly), or submit requests in anticipation of need.

DOD officials have told us of cases where contractors' employees had security clearances that were in excess of the number needed to perform on classified contracts. Over the years, audit reports by the military services have identified situations where an excessive number of security clearances were being requested for military personnel. DOD recognizes the problem and has considered a number of options to control the proliferation of security clearances, such as authorizing a specific number of clearances to each major defense component, and charging each component and its constituent contractors for each investigation requested. DOD has also emphasized to military commanders and program managers their responsibility to keep clearance requests to an absolute minimum.

Last week, DOD took some positive steps to control the number of requests for personnel security clearances. On June 10, 1985, the Defense Investigative Service announced a "Clearance Reduction Program Within Industry." The program is designed to identify and eliminate existing security clearances that are no longer required and to tighten the procedures used

by contractors to request clearances. In addition, the Secretary of Defense ordered an immediate 10 percent reduction in the number of security clearances held by military and civilian personnel. He also formed a special panel to identify "any systemic vulnerabilities or weaknesses" identified by the recent espionage case.

Need for Improved Classification Guidance
For Contractors

The large number of security clearances is driven by the volume of classified material. In our March 1981 report, we identified instances where, because of deficiencies in guidance, training, and inspections, some national security information had been improperly classified--both overclassified and underclassified--and had not been properly marked to protect it. We reviewed 235 classified documents to determine if various portions of the documents were classified correctly. Of the 235 documents, 119, or about 51 percent, contained one or more examples of improper classification. Of the 119 documents, 109 had portions that were overclassified and the other 10 had portions that were both underclassified and overclassified. In addition, we found that 90 percent of 496 documents that we reviewed, were not marked correctly to protect national security information.

We found that classification guidance furnished by DOD was outdated, vague and inconsistent. We recommended that DOD improve the classification guidance given to contractors, expand the training of contractor employees, and include classification management in its periodic security inspections of contractors. DOD agreed that more training was needed, but said that a lack of funding and personnel precluded any significant expansion of its training program.

We have not done any follow-up work on this subject; however, an April 1985 report to DOD by the National Classification Management Society concluded that classification guidance, when available to industry, often was provided late and was irrelevant, inconsistent, and unclear.

- - - - -

This concludes my prepared statement. We would be pleased to respond to any questions the Subcommittee might have.

ATTACHMENT

ATTACHMENT

GAO REPORTS ON THE PROTECTION OF NATIONAL SECURITY INFORMATION

<u>Date</u>	<u>Number</u>	<u>Title</u>
12/02/74	B-132376	Personnel Security Investigations: Inconsistent Standards and Procedures
12/16/77	FPCD-77-64	Proposals to Resolve Longstanding Problems in Investigations of Federal Employees
01/30/79	GGD-78-91	IRS Inspection Service Functions: Management Can Further Enhance Their Usefulness
03/09/79	LCD-78-125	Improved Executive Branch Oversight Needed for the Government's National Security Information Classification Program
08/31/79	FPCD-79-79	Costs of Federal Personnel Security Investigations Could and Should Be Cut
09/25/79	FPCD-79-92	Status of the Investigative Program
10/26/79	LCD-80-16	Continuing Problems in DOD's Classification of National Security Information
04/11/80	LCD-80-51	The Central Intelligence Agency's Handling of Mandatory Review Requests Under Executive Order 12065
10/15/80	LCD-81-3	Systematic Review for Declassification of National Security Information--Do Benefits Exceed Costs?
12/16/80	LCD-81-13	Oversight of the Government's Security Classification Program--Some Improvements Still Needed
03/23/81	PLRD-81-3	DOD Should Give Better Guidance and Training to Contractors Who Classify National Security Information
09/15/81	GGD-81-105	Faster Processing of DOD Personnel Security Clearances Could Avoid Millions in Losses
07/08/82	GAO/GGD-82-56	The Department of Justice Needs to Address the Problem of Two Personnel Investigations Being Conducted on All Bureau of Prisons Employees
10/07/82	GAO/GGD-83-15	Review of Department of Defense Investigation of Leak of Classified Information to <u>The Washington Post</u>
02/18/83	GAO/GGD-83-43	Further Improvements Needed in Department of Defense Oversight of Special Access (Carve-out) Contracts
05/18/83	GAO/GGD-83-66	Need for Central Adjudication Facility for Security Clearances for Navy Personnel
10/18/83	GAO/NSIAD 84-26	Effect of National Security Decision Directive-84, Safeguarding National Security Information
06/11/84	GAO/NSIAD 84-134	Polygraph and Prepublication Review Policies of Federal Agencies

BEST COPY AVAILABLE

Mr. ENGLISH. Thank you very much, Mr. Thurman. I think that was a fine statement and I appreciate your including the information that you felt needed to be highlighted.

I know Supreme Court Justice Potter Stewart once observed that when everything is classified, then nothing is classified, and the system becomes one to be disregarded by the cynical and the careless. Do you agree with that sentiment? Does that fit in line with what you have seen taking place as far as classified material is concerned?

Mr. THURMAN. I would certainly agree, Mr. Chairman, that one of the things we have to guard against is overclassification. Otherwise, classification does lose its significance for the people who have to work with it on a day-to-day basis.

The question of whether or not we face an overclassification problem and the magnitude of that problem is difficult to answer. As I alluded to in my statement, our work has indicated that there certainly are cases where material appears to be overclassified, based on the existing criteria and guidance. The magnitude of that particular phenomena is almost impossible to determine. We have not come up with an acceptable way to quantify it.

Mr. ENGLISH. Well, in your statement——

Mr. THURMAN. Yes, sir.

Mr. ENGLISH [continuing]. You highlighted for us, you were referring to Department of Defense contractors offices in which they had over 235 documents, and 51 percent of those were not classified properly.

Could you give us a little—flesh out a little more, give us a little more detail on it?

And the other question I have about that as well, you were mentioning some were overclassified and some were underclassified. What was the greatest proportion, was that fairly evenly divided or most overclassified or most underclassified?

Mr. THURMAN. The tendency we observed was more in the direction of overclassification as opposed to the underclassification problem. I might mention, too, in trying to respond fully to your question, that in about that same time period—in fact, let me get the exact data. In a report we issued in 1979, we focused on classification practices at 23 Department of Defense installations worldwide and did a very similar kind of analysis. We looked in that particular case at 556 documents and found that 133 of those documents contained information that we concluded had been improperly classified. We found information that was not related to national security, that had been classified.

References to classified documents that did not disclose classified information were classified. We found that on occasions, the same information was classified inconsistently. And, finally, information that had lost some of its sensitivity had not been downgraded.

We also found, in examining those documents, that there were marking errors—in other words the way in which the document itself is actually marked—on 33 percent of the documents. Such things, as the marking not showing the original classification authority or the office of origin, the date, or the event that should trigger the declassification review.

In the case of our work at the contractors' plants, I think our fundamental conclusion there was that, in many cases the guidance that the Department was giving to the contractors was not clear or was vague and led to some of the classification errors that we observed at the contractors' facilities.

Mr. ENGLISH. Could you give me a rough breakdown then of the percentages. Were most overclassified or most underclassified?

Mr. THURMAN. Most were overclassified. Let me give you the exact numbers if I can. Of the 119 documents, 109 had portions that, in our view, were overclassified. The other 10 had portions that were both underclassified and overclassified. So, the preponderance was to move toward the overclassified side of the equation, Mr. Chairman.

I think it is fair to say, we have observed in our work a somewhat understandable tendency to be safe rather than sorry in making classification judgments.

Mr. ENGLISH. Did you run into the same things with the Department of Defense? Is it the same sort of picture there?

Mr. THURMAN. Yes, sir.

Mr. ENGLISH. The overwhelming majority was overclassified?

Mr. THURMAN. Yes, sir; about 24 percent contained classification errors. We may have to submit those numbers for the record if we could, Mr. Chairman.

Mr. ENGLISH. Go ahead and I will ask you another question.

Does it follow then that documents or portions of documents were classified top secret when they could have been classified secret—then that would require a person with top secret clearance in order to work with those documents?

Mr. THURMAN. That is correct.

Mr. ENGLISH. So does it follow then that the more overclassified that you have, the more of a problem that we have in that area, it leads to more requirements for higher classification security clearances?

Mr. THURMAN. Yes.

Mr. ENGLISH. So, this feeds on itself?

Mr. THURMAN. Yes sir.

Mr. ENGLISH. OK. It is my understanding that the President of the United States, through Executive order, determines how something is to be classified. He sets the ground rules as to how these classifications have been carried out. Each President since Harry Truman, I believe, has been trying to narrow that definition down as to what this rule of thumb should be. So whether something should be classified or not classified, it is still a very tough interpretation to make.

Does the vagueness of that rule, or the lack of it, is that having an impact as to whether or not some of this material is being overclassified or not?

Mr. THURMAN. Mr. Chairman, you are asking an extremely good question, and I think a very tough one to answer in any sort of factual, analytical way. There is no question in my mind that there is a great deal of judgment involved in the entire process on when a particular piece of information requires protection.

The basic process that is in place—I would ask Mr. Boker if he would like to expand on anything that I leave out here—the basic

process that is in place to make classification judgments rests with something like 7,000 or so individuals throughout the Federal Establishment who have the so-called delegated responsibility, that you referred to, to make original classification determinations.

That in turn, works its way through the bureaucracy, through, for example, in the case of the Department of Defense, through the use of classification guides. So, if you or I are working in the program office of a particular weapon system, we will be working with classification guides to determine whether the information that we are producing as part of our day-to-day execution of our job is, in fact, classified.

The same sort of process takes place with respect to defense contractors. The defense contractors have no original classification authority. They exercise, or perform, their classification of documents using guides that are furnished by the Department of Defense and, in that process, there is no question that judgment is involved.

I think in my years with Government, I have seen, as I am sure you have, sir, the swing in the pendulum between emphasis on strengthening of our classification system, and then on occasion, we will see a loosening of it.

I suppose we will always be faced with something of a dilemma. What is one man's needed classification, in order to protect vital information, might be another's coverup to forestall public scrutiny of a particular transaction. That dilemma seems to be inherent and just part of this entire process.

Mr. ENGLISH. I am going to try to tie you down tighter. I think to keep it in perspective, we have narrowed down considerably the number of people who have the responsibility for classifying information. In 1972, we had around 60,000 people with authority to classify information, and as you accurately pointed out, we now have somewhere between 7,000 and 8,000. So there has been a reduction.

By the same token, while we have also tried to narrow down the focus of the Executive order—until recently, that is, we have been trying to narrow the scope—there is another point that I think we want to keep in mind, and that is the changes of a word or two can make a big difference. On the previous Executive order with regard to the manner in which someone should decide whether to classify information or not, we had the words "identifiable damage to national security."

At the present time, under the regulation and Executive order, the word "identifiable" has been removed and it is simply "damage to national security." Do you find that it is easier, or I guess from the standpoint you could say more difficult, in making that decision for these 7,000 to 8,000 people with the removal of that word? In other words, does that broaden the scope of the information that falls in the purview to be classified and gives much less direction?

Mr. THURMAN. On that particular question, Mr. Chairman, we have not looked under the current order at classification actions that are being taken. So, quite frankly, I am not in a particularly good, or not in any, position to respond in any sort of factual way to your question.

As a personal judgment I would think, yes, it would send a certain signal that would change the mindset of the person faced with

making that judgment. But we don't have, at least to my knowledge, any data to respond in a factual way to your question.

Mr. ENGLISH. Utilizing the time in which you made a study, I assume that you talked to many of the people who had this responsibility of classifying material. Did you find a good deal of doubt in their minds, did they express the fact that they lacked guidelines, that they felt they were strict enough, and that they were uncertain? Did you find that was expressed at all?

Mr. BOKER. Our most detailed review was in industry and, of course, industry relies upon guidance furnished by the Government, and the biggest problem was that the guidance was not forthcoming, or was unclear. So, the individual charged with marking a document secret or top secret didn't know what he was supposed to do.

There are well over a thousand classification guides produced by the Department of Defense for various systems, operations, and plans and these are what an engineer uses when he has a problem of how to mark a document. We asked an individual why a document was marked in such and such a way and had him refer back to the classification guide. That is where we found most of the errors. They didn't have the guidance or they were not following the guidance given, or it wasn't clear as to how they should mark a document.

Mr. ENGLISH. Did you find cases in which people were classifying documents because they wanted to bring it to the attention of superiors?

Mr. BOKER. No, we found cases where they were trying to prevent embarrassment in the military, something they shouldn't have been doing. A few of those, but not too many. Primarily, they were just mistakes. We didn't see anything that looked like it was deliberately marked to mislead somebody except in a few cases.

Mr. ENGLISH. Mr. Lightfoot.

Mr. LIGHTFOOT. Thank you, Mr. Chairman.

I have several questions, Mr. Thurman, about the national agency check and inquiries and personnel security examinations for those seeking top secret clearances. Does the NACI require contact with local law enforcement authorities for information about the applicant?

Mr. THURMAN. No, sir. The national agency check itself consists of going to Federal agencies such as the Department of Justice, FBI, the Department of State, and so forth. The so-called local agency check is not a part of the national agency check.

Mr. LIGHTFOOT. Would it be helpful?

Mr. BOKER. Definitely. Not all local agencies report information to the FBI.

Mr. LIGHTFOOT. Are there legal obstacles involved in obtaining information from local agencies or do you need consent from the applicant to go ahead and do that in the first place?

Mr. THURMAN. Congressman Lightfoot, about 5 or 6 years ago, we recommended that the Congress give serious consideration to new legislation in the whole area of personnel security clearances to try to come to grips with some inconsistencies. I don't want to give you too long an answer here, but to try to come to grips with

BEST COPY AVAILABLE

inconsistencies between the current Executive order that governs Federal employees as well as contractor employees.

One of the areas that we thought that legislation might help to address was to provide a clear basis for the Federal Government to have access to the law enforcement records of local agencies. I don't think it is all that much of a problem, but, on occasion, it has surfaced as an issue in doing the background investigations. In other words, just the legal right of the Federal Government to have access to the records of local law enforcement agencies.

Mr. LIGHTFOOT. What about financial and credit history? Many people, it seems to me, for financial reasons, sometimes stray off the beaten path. Can you check into that and, if so, is that kind of information available to background investigators? Do you feel it should be if it is not now?

Mr. BOKER. Well, we are talking about, first of all, a national agency check with inquiries, that is only for secret clearances. A top secret clearance requires a national agency check and background investigation. That would involve a local agency check, as well as a credit check and other checks that are done at this point in time. The majority of people with clearances in the Government and industry have secret clearances. The more detailed investigation or background investigation can only be done for those individuals who need a top secret clearance or special access.

Mr. LIGHTFOOT. It is my understanding you go back 5 years, the NACI goes back 5 years, FBI goes back 5 years, special background goes back 15 years.

Mr. BOKER. A national agency check goes back as far as the records may go.

Mr. LIGHTFOOT. You are satisfied that that is far enough in all cases?

Mr. BOKER. We are not satisfied with anything right now.

Mr. LIGHTFOOT. In your prepared testimony you said there is a need to continuously monitor cleared individuals. Specifically you said that Government agencies and contractors need to pay close attention to employees with emotional or drug-related or severe financial problems.

You went on to say you found agencies reluctant to revoke clearances, since revocation might be considered an adverse action. Could you elaborate on that for us a little bit, first describing the procedures which supervisors must follow if they suspect an employee is suffering from one of those problems you mentioned?

Mr. THURMAN. One of the issues that people who work in this field as professionals, on a daily basis, talk about as much as anything else, is the need for a supervisor to observe changes in behavior patterns, that might lead one to suspect that action should be taken to consider whether or not the individual should retain a security clearance.

The process that is used, as I understand it, is that a supervisor who observes, for example, an employee whom he suspects of having a drinking problem, or a drug-related problem, has an obligation to report that to his or her agency security office. That action can lead to a special investigation that may be initiated to determine the employee's suitability for continuing to have a security clearance.

Agencies sometimes appear reluctant to revoke a security clearance, because it is a rather somber responsibility, in that such action can affect a person's ability to earn a living. I know in my own job, I have had some cases come to me dealing with particular problems that an individual has encountered and judgments have to be made on whether or not that particular pattern of behavior does seem to warrant the rather drastic step of revoking a security clearance and prohibiting that person from carrying out his or her job or assignment.

I think it is that kind of pressure that causes the pattern that you often see of Federal agencies, rather than pulling the clearance, simply moving a person into another assignment where the individual will not have access to classified information.

Mr. LIGHTFOOT. One last question, a quick followup on what you just said. How diligently do you feel supervisors are in following up in this type of thing and moving that person or removing that person, as the case might be?

Mr. THURMAN. I will offer a personal judgment based on my own role as a manager in the Federal Establishment. I think it is an area that all of us need to pay more attention to.

Mr. LIGHTFOOT. Thank you.

Thank you, Mr. Chairman.

Mr. ENGLISH. Mr. Neal.

Mr. NEAL. Thank you, Mr. Chairman.

Is there a good correlation between these problem areas that you list and the problems with leaking security information?

The reason I ask that, I just, in reading about Mr. Walker, I don't recall reading that he had an alcohol or drug problem or severe financial problems. It seemed to me it was something else, although maybe you can comment on that.

Mr. THURMAN. The question of correlation is an excellent one. I am not personally aware of any studies that have been done of the correlation between the kinds of things that are covered in a background investigation or a security investigation and—

Mr. NEAL. In the problem area. I think it is important somehow we look into that. I recall Mr. Winston Churchill drank rather heavily and yet I believe it would have been a mistake to deny him a security classification.

The other area in these checks, you didn't mention lie detectors, are they relied upon heavily?

Mr. THURMAN. The polygraph is used. It is my understanding that the polygraph is used to some extent in the screening that is done for the intelligence agencies. We have some numbers on the use of the polygraph that we would be happy to provide for the record.

Mr. NEAL. It seems to me I have read recently the Reagan administration intends to increase dramatically the use of the polygraph. Let me tell why I raise that question.

We had testimony before another Government Operations subcommittee a couple of years ago to the effect that the polygraphs were no better in detecting lying than the flip of a coin. Obviously, the fact is they don't detect lying. They detect emotional changes, and that some people can beat the polygraph rather consistently and some become emotional to a point that it would indicate a

problem if one were to say that high emotion indicates lying when they are telling the truth.

So, according to this testimony which I found to be very impressive, if you depend on the polygraph, you run a very high risk of clearing some people who are skillful liars and convicting people who are innocent because they are not very good at taking these polygraph tests.

Mr. THURMAN. Congressman Neal, I think our only real response to that is we have not done any independent evaluations of the veracity of the polygraph technique, and I am aware of the disagreements that exist—

Mr. NEAL. How helpful?

Mr. THURMAN. On the use of the polygraph and—

Mr. NEAL. Could you tell me how much weight the polygraph is given in these kinds of investigations, the kinds that you are testifying about today?

Mr. THURMAN. Very, very little is the answer as far as the normal background investigation is concerned. The polygraph is used to some extent on the screening for the so-called SCI access, involving access to intelligence methods and sources and so forth, but not in the Defense Investigative Service investigations.

Congressman Neal, we could submit some material for the record because we do have some statistics on the use of the polygraph over, I believe, it is the 1977-83 timeframe.

Mr. NEAL. I would like to see that. Does that deal with the rate of increase in the use also?

Mr. THURMAN. If memory serves me right, I think we did see an increase from 1981 through 1983. I believe, as part of the Defense Authorization Act of 1985 there was a ceiling of 3,500 put on the use of the polygraph by the Department of Defense. I believe that limitation excluded NSA and CIA.

Mr. BOKER. Yes, sir; that was a 3,500-person test, as opposed to the use of the polygraph for criminal investigations and counterintelligence inquiries where its use is authorized by DOD's directives. The Department wanted to use the polygraph for screening purposes, before a person is given access to a sensitive program.

I am aware of the hearings you are referring to. Two years ago, we provided the information to the Subcommittee on Legislation and National Security. If you already have that data, we have nothing new since then.

Mr. NEAL. You used the term "improperly qualified."

Mr. THURMAN. Yes, sir.

Mr. NEAL. It sounds to me like that would be a very judgmental kind of term to use since the guidelines are clear, as I understand your testimony.

Mr. BOKER. In those cases, the individuals responsible for classifying the documents agreed with us. It was not our judgment. We said, here is the classification guide. Why did you classify it this way? If there was no guide, why did you classify it a certain way?

The individual who did the classification acknowledged that it was wrong. It is not our judgment. We are not experts in the field.

Mr. NEAL. I am just wondering. The chairman tried to get into this area when we are classifying too much or too little, and so on, I certainly understand the tendency to want to be safe rather than

sorry. Maybe you have already said this, and I didn't understand it clearly, but as a result of President Reagan's Executive order issued in April 1982; have the number of classified documents gone up significantly?

Mr. BOKER. I believe the number has gone up, according to the Information Security Oversight Office's reports. I don't think it is a significant number, but the annual report put out by the Security Oversight Office does show moderate increases.

Mr. ENGLISH. Will you yield?

Mr. NEAL. Sure.

Mr. ENGLISH. But I think it is also important to point out that the number of instances in which something was classified does not relate to when we are talking about a single page, a single paragraph, or an entire report or a book for that matter. So I think in order to keep it in perspective, it is important that if one is asking the question about volume and amount, that that particular piece of information could be misleading.

I don't know what the answer is either, but I think it is important to know these were specific instances in which something was classified whether it was a single sentence, paragraph or hundreds of pages.

Mr. THURMAN. Yes, sir.

Mr. NEAL. Counsel points out the distinction between a decision and the number of pages or something. The question really has to do with the number of decisions, not the actual number of pages or words.

Mr. BOKER. We have no data, but the Information Security Oversight Office puts out an annual report with the data. I don't know what the distinction is, if it is a decision—

Mr. NEAL. We will look at that.

Mr. BOKER. They have original decisions and derivative classifications. So, there is a difference there.

Mr. NEAL. I just have two other questions. One has to do with the general feeling I have that although the kinds of investigation you are talking about that we use in the various agencies of Government are probably necessary and so on, but I am wondering if they really get at a situation like that situation here with Walker and his associates. I just don't recall. He had an alcohol problem and that is the reason that he started selling documents—or a drug problem, or unique financial problems.

Everyone has financial problems. Or that he told the truth or not in the case if the polygraph was involved. Are we going to be able to uncover problems like this in advance of their occurring using the techniques that we are now using?

Mr. THURMAN. I will ask the gentlemen with me to also respond because I think it is the crucial question. My own reaction from everything I have read and seen from both our own work, as well as the work of others, I am not sure there is a foolproof or—

Mr. NEAL. I am not asking you to come close to it. Are we on the right track is my basic question. There are other possibilities, for instance, I don't know how reliable it is. I haven't looked at it in years. Psychological testing may be able to produce some good results. I don't know.

Mr. REID. One of the problems in the Walker case is it wasn't a typical case. The all American family, no matter what kind of reinvestigation we have in place now, no matter what we would have done, would have caught the people involved in the Walker case.

The son has a secret clearance. There is no requirement for a secret update. They never would have caught him.

Mr. NEAL. Even if there had been a requirement for an update, what would you have learned? All American type, no drugs, no drinking, no unique—

Mr. REID. Not a lot, and when the uncle and father were in the Navy, there was no requirement for an update of a top secret clearance for members of the military.

Mr. NEAL. Let's say you have gone through these procedures. Wouldn't you have gotten the update?

Mr. REID. Yes, but it wouldn't have done any good. This is an atypical case. We haven't examined the other cases.

Mr. NEAL. I asked this question about correlation between these elements and spying. You say this was atypical?

Mr. REID. In other cases some are heavy into alcohol or have a lot of financial difficulties. If that is brought up in a credit check, maybe they would look at the person closer, and they should.

Mr. NEAL. Is there a correlation with that and selling secrets?

Mr. REID. I am not sure we—

Mr. NEAL. If there is not, why are you looking at it? It may be valuable for some other reason. Is it valuable? The question is, is it valuable to look at these things if there is no correlation between things and selling classified information?

Mr. BOKER. I think in the Bell and Harper cases, financial difficulties and alcoholism, were factors. I think in most cases the indicators were there. They were not checked too carefully. The Walker case is unique in that none of the indicators would have indicated a problem that these were potential traitors. In the other cases, most of the indicators were present and, if properly investigated, would have disclosed the possibility of a compromise of national security information.

Mr. NEAL. We need to do some more work in this area. One last question. On page 6 of your testimony you say that we found the classification guidance furnished by DOD was outdated, vague and inconsistent. We recommended that DOD improve the classification guidance given to contractors, expand the training of contractor employees and so on. Then you say DOD agreed that more training was needed, but said that a lack of funding and personnel preclude any significant expansion of its training program.

Does that mean that we are doomed to live with this situation from now on?

Mr. THURMAN. Perhaps I can answer that question, by providing something of a brief oversight of the Defense Investigative Service and where it has been. Back in the early 1980's, as we mentioned earlier, the service ran into some fairly significant backlog and timeliness problems, because of the volume of security clearances that were being requested.

We, back at that point, supported an increase in the level of staffing for the service. The investigative time, as a result of the

increased staffing, which the service obtained in about 1983 or 1984, showed some improvement.

It is a long way of answering your question. But, the fact of the matter is, the resources that we have brought to bear in this particular area have been constrained. They were badly constrained, in our view, back in the early 1980's.

The agency was faced with extremely large backlogs in just getting the investigative workload handled, and tradeoffs had to be made between the amount of effort that could be devoted to training versus that workload.

Mr. NEAL. What happened to their budget request for this?

Mr. THURMAN. The staffing for the service was increased by about 600 people, I believe, wasn't it, 600 investigators in 1983?

Mr. BOKER. 1982 and 1983.

Mr. THURMAN. So there was an increase in 1982 and 1983.

Mr. NEAL. And this statement represents the situation before that time?

Mr. THURMAN. Before that time, yes, sir, that is correct.

Mr. NEAL. They had gotten what the Congress had asked, I assume. I assume that.

Mr. BOKER. They reprogrammed money within DOD. I think we are confusing two things here. We are talking about the training of people who classify documents, as opposed to investigators who conduct personnel security investigations prior to the granting of security clearances.

They are two different matters. I think we have overlapped the two. As far as training goes, I don't recall that they have had a major increase in funding. There has been great emphasis placed on training within major DOD components, particularly in the military.

They have taken more interest in the area and have tried to provide more training. It is still inadequate, because you are talking about many, many people. As far as the investigators go for personnel security investigations, they were increased by about 670, at an increase in cost of about \$20 to \$28 million, between 1982 and 1983.

Mr. NEAL. I thank you. I thank all of you.

Mr. ENGLISH. Mr. Miller.

Mr. MILLER. Yes, Mr. Chairman.

Gentlemen, given that we have resource limitations, if you were to recommend setting priorities, looking at some of the choices, for example, boosting the resources going to initial background checks or to the national agency checks and inquiries, or to the reinvestigation process, what would you recommend should be the first priority among those three or others in the allocating of resources?

Mr. THURMAN. It seems to me, Mr. Miller, and the other two gentlemen here can express their judgment on that, too, and it is strictly a personal judgment, that the important areas of focus for additional effort should be on those individuals that have access to the most sensitive of the Nation's classified materials, those at the SCI level or at the top secret level would be your first order of priority for increasing attention and investigative focus.

I would start by focusing in that area.

Mr. MILLER. Investigations?

Mr. THURMAN. Yes; in other words, trying to get as current as we possibly can on the periodic reinvestigations of those holding top secret clearances and SCI access. That would be my initial priority.

Mr. MILLER. Is there agreement on that?

Mr. REID. I agree. The reinvestigation is probably the most important part. It is not when individuals first receive clearances that they are going to have the financial problems. They are usually young, entering the service or Federal employment and just out of college. They get their clearances and they can go for 20 years without a reinvestigation. It is when they have children in college, large mortgages, and other major commitments that require the focus of attention.

That is when people tend to get in trouble and not just at the beginning of their careers.

Mr. MILLER. Thank you.

Mr. ENGLISH. Thank you.

Mr. Spratt.

Mr. SPRATT. No; thank you, Mr. Chairman.

Mr. ENGLISH. Mr. Thurman, I have additional questions for you. I will submit those in writing, if we might. We would appreciate a timely response.

I want to thank you all for your cooperation.

Mr. THURMAN. Thank you, Mr. Chairman.

Mr. ENGLISH. Our next witness will be Mr. Philip A. Parker, Deputy Assistant Director for the Intelligence Division, Federal Bureau of Investigation.

I assume you are the nuts and bolts man with regard to counter-espionage, is that correct?

STATEMENT OF PHILIP A. PARKER, DEPUTY ASSISTANT DIRECTOR, INTELLIGENCE DIVISION, FEDERAL BUREAU OF INVESTIGATION, ACCOMPANIED BY HARRY PORTER, SPECIAL AGENT

Mr. PARKER. Yes, sir; I would like to think that.

Mr. ENGLISH. We would be happy to receive your testimony. If you would care to abbreviate your testimony, without objection, your full and complete testimony will be made a part of the record. We will be happy to have you summarize.

Mr. PARKER. It is pretty much abbreviated already.

Mr. ENGLISH. Fine, go ahead and give it.

Mr. PARKER. Seated to my left is Special Agent Harry Porter, the Unit Chief in our Intelligence Division.

Mr. ENGLISH. I might state, before we take off fully on this, we recognize the fact that the Walker case is an ongoing case, and that you cannot get into the details of that specific case, so we will try to have our questions in those areas that would be of general information. And, also anything that would be of a classified nature, we would ask you to identify that in any answer that would have to be classified, so that we could hear it in closed session.

Mr. PARKER. Thank you.

Mr. ENGLISH. Thank you, sir.

Mr. PARKER. Mr. Chairman, Congressmen, I am here today to provide to this subcommittee background regarding the FBI's responsibilities to investigate violations of the espionage laws and to conduct foreign counterintelligence investigations in the United States.

I would like to begin my remarks by discussing the nature of the threat, the FBI's jurisdiction, the mission of hostile intelligence services, some recent cases, and describe what the FBI is doing to counter hostile efforts.

In his remarks before the House Permanent Select Committee on Intelligence in March 1985, Judge Webster pointed out that there are over 4,300 officials in the United States assigned to over 220 Soviet, Soviet bloc, Cuban, and other Communist diplomatic and commercial facilities. Over 30 percent of the officials are known or suspected intelligence officers.

Judge Webster also commented on the dozens of intelligence officers with specific Capitol Hill assignments seeking political and military intelligence.

In the past 10 years, hostile intelligence services have become increasingly aggressive. We believe this stepped-up activity is due to the virtual explosion of technological advances in the scientific community, the defense establishment and the private sector.

JURISDICTION

The FBI's goals, duties and responsibilities with respect to the national counterintelligence effort derive from the President's power to conduct foreign relations. In addition, our authority includes investigations of violations of espionage and related laws.

On December 4, 1981, President Reagan issued Executive Order 12333, "United States Intelligence Activities." Section 1.14 delineates the FBI's responsibilities. It replaced similar orders issued by Presidents Carter and Ford.

Pursuant to section 1.14, the FBI has primary responsibility for conducting foreign counterintelligence investigations within the United States. These investigations are conducted under the supervision of the Attorney General, and in accordance with the Attorney General's guidelines for foreign intelligence collection and foreign counterintelligence investigations.

The FBI also coordinates the counterintelligence activities within the United States of other agencies of the intelligence community. The coordination is generally done through memoranda of understanding or other agreements between the Attorney General and the heads of such intelligence agencies.

There are a number of techniques used in carrying out our investigative responsibilities. The principal approach, interviews, solicits information from cooperative citizens. In certain cases, physical surveillances are employed. And in a limited number of cases where other investigative means are inappropriate, electronic surveillance is used.

Pursuant to authority set forth in the Foreign Intelligence Surveillance Act of 1978, title 50, United States Code, sections 1801-11, Public Law 95-511, the FBI conducts electronic surveillance of cer-

tain hostile foreign powers and their agents within the United States.

The applications for such surveillance are prepared by the Attorney General's staff, and incorporate the FBI's affidavit justifying the request for surveillance.

The applications are then approved personally by the Attorney General and submitted to the Foreign Intelligence Surveillance Court. The judge receiving the application either approves or disapproves the surveillance.

Collection mission of hostile intelligence services:

The collection mission of hostile intelligence service officers in the United States includes the assessment and recruitment of Americans as agents. Hostile services are constantly in contact with our citizens, evaluating them as potential sources of information.

The methods used to recruit individuals who obtain sensitive information vary. In a very few cases, a disgruntled or mentally disturbed person volunteers information during a visit to one of the hostile foreign consulates or missions in this country.

In some cases, commercial establishments are used as cover mechanisms to acquire material, the end user may not be known to the U.S. businessman. In other cases, hostile services seek to identify people with financial or professional problems that might make them especially vulnerable to exploitation.

Revenge, ego, and financial need or greed motivate people to do many things, the most damaging step they can take is to commit espionage.

Case examples:

In the past 10 years, there have been a number of espionage cases that illustrate just what we are talking about today. I would like to summarize several of these cases to give you an idea of how difficult it is to control sensitive information.

James Harper, with no security clearance, used his contacts in Silicon Valley to gain access to classified documents and restricted material. This material included extremely sensitive information relating to the Minuteman intercontinental ballistic missile system, and the ballistic missile research and development programs of the United States, which he passed to the Polish intelligence service in Europe. How was Harper able to obtain this information?

Harper wanted money and he voluntarily chose to assist the Polish intelligence service. He used his wife, now deceased, to acquire documents to which she had access by virtue of her position with a defense contract facility.

He was paid handsomely, some \$250,000, by the Polish intelligence services. His wife was able to obtain documents routinely, although she had no need to know any of the information contained in the documents, because she was the personal secretary for a senior officer in the company, and no one questioned her need for documents.

It was, frankly, a very straightforward, simple approach to acquiring very sensitive information.

Thomas Patrick Cavanagh:

Thomas Cavanagh was an engineering specialist with a major west coast defense contractor. He wanted money and he contacted the Soviets and arranged to meet with them to sell classified documents.

What he did not bargain for was that our agents became aware of these plans and recontacted Cavanagh representing themselves to be Soviets. A meeting was arranged and Cavanagh requested \$25,000 in cash for certain classified information. A second meeting was arranged, during which Cavanagh passed classified information to our agents. He was arrested.

Alice Michelson:

Alice Michelson, a 67-year-old East German national and school-teacher, was arrested by the FBI in October 1984 as she prepared to depart the United States for Prague, Czechoslovakia, and East Berlin.

Michelson was being used by the KGB to courier documents. We believe she was employed because her age and appearance were unlikely to raise suspicions. An older woman and an academician, any suspicions raised would be easily dismissed.

We were able to neutralize this situation through the cooperation of a U.S. Army sergeant who had been asked by the KGB to work for them, but who reported the contact to the Army Intelligence Command.

Ernst W. Forbrich:

Ernst Forbrich, a West German citizen and manager of a gasoline station outside a U.S. Army base in West Germany, had frequent contact with U.S. servicemen. The FBI learned in July 1982 that Forbrich and a U.S. serviceman had engaged in espionage while the latter individual was stationed in West Germany, and continuing after that person's retirement from the service.

Forbrich was arrested shortly after he accepted classified documents from an undercover FBI agent while on a visit to the United States.

Brian Patrick Horton:

Brian Horton was an intelligence specialist in the U.S. Navy with top secret clearance, and assigned to a very sensitive area concerning U.S. nuclear war plans. The FBI learned that Horton was in contact with a Soviet military office in 1982.

The FBI immediately established contact with the Naval Investigative Service [NIS], and a joint operation was initiated. Horton was subsequently confronted with evidence of his activities, and he denied providing classified information to the Soviets.

He was subsequently court-martialed, pleading guilty to unauthorized contact with the Soviets, and found guilty of soliciting a Soviet to commit espionage.

What the FBI is doing to counter the threat:

For many years, our special agents in their daily contacts with Government and private industry, including the defense contractors, have discussed the hostile intelligence threat.

We have encouraged people to report unusual or suspicious activities on the part of persons involved in sensitive employments.

We are convinced that our best defense against hostile intelligence activities in this country rests on a cooperative citizenry, a

well-informed citizen, someone who chooses to become involved when the best interests of the country are threatened.

In 1976, one of our field divisions created a program to systematically contact all of the defense contractors within that office's territory. These contacts were to alert contractors to the threat posed by hostile intelligence services, and to give them a point of contact should unusual activity come to their attention.

In 1978, this program was formalized, development of counterintelligence awareness, [DECA], and implemented in all of our field offices. In 1984 alone, some 6,700 Defense-cleared facilities were contacted under the Deca Program.

Indeed, the program has resulted in some important information that may not have otherwise come to our attention.

Thousands upon thousands of classified or otherwise sensitive documents are produced in the intelligence community, the defense establishment and private contract facilities. Safeguarding these documents and insuring that the people handling them are not agents of a foreign power is critically important.

The responsibility for this effort rests with each of the countermeasures and personnel security components of each agency in the U.S. Government.

Despite the information that finds its way into the hands of a hostile intelligence service, despite those people who choose to commit espionage, there still remains the vast majority of citizens who do not permit themselves to be compromised or engage in activities harmful to the United States.

It is for those people that we must balance our response to the hostile intelligence threat in the United States. Countermeasures and counterespionage are relatively easy problems to solve in a totalitarian state; but this is not a totalitarian state.

The FBI believes, as does the rest of the Federal Government, we must continue to enhance our counterintelligence and countermeasures programs without encroaching on the personal liberties of our citizens.

Mr. Chairman, that concludes my remarks.

Mr. ENGLISH. Thank you very much, Mr. Parker. I mentioned in my opening statement that the modern spy, for the most part, is not recruited. He offers his services. Would you agree with that assessment?

Mr. PARKER. Yes, sir.

Mr. ENGLISH. So in effect, it is U.S. citizens going to either Soviet nationals, to the Soviet Embassy or to some other Eastern bloc country which they know they can make contact with, and that is really where the initial relationship begins. Is that the manner in which you see it?

Mr. PARKER. Yes, sir, I think that is basically the problem as we see it.

Mr. ENGLISH. And I also mentioned, now we have around 4,000 Soviet nationals in this country.

Mr. PARKER. No, sir, that is 4,000 total Communists, Soviet bloc, Communists.

Mr. ENGLISH. Soviet bloc and Soviets in this country. It would seem to me then, given the tendency, the trend that we have at the present time, the most productive way in which you can conduct a

counterespionage program is to keep careful eye on who contacts those people from those countries.

In other words, if you end up with whoever goes up and contacts the Soviet Embassy, for instance, that would be a person that you might want to take a look at, you might want to evaluate, particularly if he has a security clearance, would that be correct?

Mr. PARKER. The investigative techniques that we use against the hostile intelligence services include talking to Americans who are in contact with those establishments. We greatly depend on the cooperation of our citizens to give us information as to what is going on in those areas.

Mr. ENGLISH. The number of Soviet nationals and Eastern bloc country nationals in the United States—has that increased considerably over the last 10 to 15 years?

Mr. PARKER. It has increased, and on a relatively steady increase over the past 15 years, yes, sir.

Mr. ENGLISH. And has this made it more difficult, more complicated, if you will, to try to keep tabs on people who come in contact with them?

Mr. PARKER. The sheer number itself does cause problems, yes, sir.

Mr. ENGLISH. And do you have any idea of approximately how many American citizens we have in the Soviet Union?

Mr. PARKER. You mean diplomatically?

Mr. ENGLISH. All U.S. nationals.

Mr. PARKER. No, I don't have those numbers. The State Department, I think, would be able to provide those.

Mr. ENGLISH. We may have to acquire those from the State Department. It is also, of course, my understanding they don't have near the access to the Soviet Union that Soviet nationals do in this country.

Would the FBI support a policy of reciprocity from the standpoint that Soviet and Eastern bloc citizens would not be allowed any access to our country outside the same limits that they offer our nationals in their country?

Mr. PARKER. I think when Congress established the Office of Foreign Missions, it was looking at that from the point of view of reciprocity, and we fully support that.

Mr. ENGLISH. So you feel that Soviet nationals and Eastern bloc nationals should not have any greater access to this country in any greater numbers than they allow United States citizens to their countries?

Mr. PARKER. That is correct, yes, sir.

Mr. ENGLISH. Also, it has been my understanding, and I hope that you will correct me if I am in error, but particularly through the sixties and perhaps on into the seventies, there was a deemphasis as far as counterespionage as far as the U.S. Government is concerned, is that correct?

Mr. PARKER. I worked during that period, and I don't know that there was a deemphasis during that time insofar as counterintelligence is concerned. I do know that over the past 10 years, there has certainly been increased interest in the FBI and our own training, our own ability and our own manpower, and I think the result of those efforts has been shown.

Mr. ENGLISH. Has it increased in the same proportion and at the same rate as has the number of Soviet and Eastern bloc nationals in this country?

Mr. PORTER. I would say no, sir, it has not.

Mr. ENGLISH. It has not increased at that rate?

Mr. PORTER. I doubt that we would be able to increase that rapidly.

Mr. ENGLISH. Have we gotten to the point that as far as Soviet and Eastern bloc nationals are concerned in this country, and given the access that they have to this country, that there are just simply too many of them scattered out over too great an area to keep track of?

Mr. PARKER. Well, their locations are mainly New York, Washington, San Francisco, and Chicago, which, of course, is where we have our larger concentrations.

Mr. ENGLISH. But they can move out about the country any time that they wish. Any Communist diplomat here in the United States, with a few exceptions—I understand there may be a few exceptions—basically they can drive off down to Richmond any time they want to, or if they want to go to Charlottesville, they can.

If they want to go to Oklahoma City, they are free to do it, is that correct?

Mr. PARKER. That is correct, with the exception of the Soviets.

Mr. ENGLISH. And again, identify if I am getting into an area here that we need to discuss in closed session, but could you tell us on an average, how many agents it would take to keep track of one Soviet citizen? I would assume that it would take far more than one?

Mr. PARKER. One Soviet intelligence officer. We have to first find out which one is the intelligence officer, and then if we tried to keep track of him for 24 hours, the numbers—it is certainly more than five, plus there is considerable support that has to be brought in there, more than just the special agent.

Mr. ENGLISH. So, in effect, if we were going to try to assume that we had complete coverage of Soviet and Eastern bloc country nationals in this country, the 4,000, we are talking about—it would take better than 20,000 people just to do that job full time; is that correct?

Mr. PARKER. That is correct.

Mr. ENGLISH. And an enormous amount of resources, so there is a tremendous multiplier effect, the greater the number of those citizens that are in this country, because you can't really be sure, you may have a pretty good idea, but you can't be dead certain that this one is and this one is not.

Mr. PARKER. That is absolutely correct. If we could bet on only the winners at a horse race, it would save our time losing money on the others. We can't do that insofar as the Soviets or the bloc people who are here.

We don't know which one is for sure an intelligence officer.

Mr. ENGLISH. But, too, if we are looking at this entire difficulty, this entire problem that we are facing, and we have 4 million people out there that have security clearances, we have over 600,000 that have top secret security clearances, then basically the best shot we have is whenever they hand that information off to a

Soviet citizen, that is where we can really narrow it down, but even then, we are talking about 4,000 possibilities.

Mr. PARKER. Yes.

Mr. ENGLISH. And so, it is a very complex equation in trying to make certain that we do have the type of coverage that is necessary to do that kind of job.

Mr. PARKER. Absolutely. You have pinpointed the critical issue. It is the point of contact, and detecting an agent for a hostile service.

Mr. ENGLISH. And that does not even include the additional complication; namely, that those citizens, U.S. citizens, could be going to some other country, Mexico or Canada or some place else, meeting outside of our borders, which further complicates the entire process.

We have a different type of spy on our hands; 30 or 40 years ago, we had the spy who was motivated by ideology. Today, we get into the greed situation. It appears, at least, that money is playing a very big role these days.

Can you give us something of a profile of what today's spy looks like?

Mr. PARKER. No profile has been determined. We have young, all-American boys such as Seaman Horton, who had all sorts of good things going for him. We have had Mr. Harper, who was pretty much well-established in his business.

We have Mr. Helmich, whom we convicted back in 1980 or 1981, who was a well-respected NCO in the Army, from all accounts that we had at the time. So today, there is not a profile, we have not come up with one to date.

We are looking into the various psychological aspects of it, to see if there is something that someone with the training that could say, is there a quirk which can point out someone who is going to take that step to commit espionage exists?

To date, we cannot say that such a profile with any validity does exist.

Mr. ENGLISH. Staff just pointed out to me that the Soviet Embassy in Mexico is Russia's second largest Embassy in the world.

Mr. Lightfoot.

Mr. LIGHTFOOT. Thank you, Mr. English.

Carrying on on your thought, I understand that the Soviets are going to build theirs on top of a hill here, which is probably a mistake.

Mr. PARKER. Yes, sir, they are.

Mr. LIGHTFOOT. The memorandum of understanding which you have with the military departments' investigative services, could you explain a little bit whose responsibility is what? What is your role, what is their role? How does that work again?

Mr. PARKER. Carrying out counterintelligence investigations inside the United States is the responsibility of the FBI. However, if we are moving into an area of counterespionage, an investigation into an espionage act, and it involves someone who is a member of the military, the military has the primary jurisdiction with that individual.

As it often happens, we get information about a contact between a military man and a hostile service. We immediately bring that to

the attention of the appropriate military service, and it normally works out that we work the case together.

We will have the interest in the hostile service and the knowledge of how that service works, who its members are, what are their techniques.

The opposite also happens. If the military finds out that one of their personnel is involved in espionage, they will come to us and we will work the case together, but the primary jurisdiction of the man or woman themselves falls within the appropriate military service.

We also conduct joint operations with the military, and counter-intelligence investigations, and I prefer not to go into that any further.

Mr. LIGHTFOOT. If I could follow up a little on one of our chairman's other questions, you are saying it takes roughly five U.S. agents to cover one of their—

Mr. PARKER. I said it would take more than that.

Mr. LIGHTFOOT. You are talking about field officers, I would assume.

Mr. PARKER. Yes, sir.

Mr. LIGHTFOOT. There was a story in one of the papers yesterday that said that the Senate Intelligence Committee has identified at least 200 KGB agents among 800 members of the Soviet delegation to the United Nations.

This was in the New York Times, and applying that formula to that, and I would assume the KGB agents would be at the top of your list as far as priorities of those that you want to keep your eye on; so, you are talking about a thousand agents in the field, plus all the support.

I realize that manpower figures and your budget are confidential, but are you undermanned? Can you handle this? I don't know how to get you to answer that without revealing something you shouldn't, but I think that is a very important question.

Mr. PARKER. Undermanned but never outfought.

Mr. ENGLISH. Will the gentleman yield at that point?

Mr. LIGHTFOOT. Certainly.

Mr. ENGLISH. This might be an interesting point. If it is classified, say so, but can you tell us the total number within the entire FBI, the number of agents that you have in the FBI to do the whole job, all law enforcement as well as counterespionage, ball park.

Mr. PARKER. No, sir. I would prefer to discuss any figures such as that—

Mr. ENGLISH. All right, we will get into that in closed session, but I thank the gentleman for making a good point there.

Mr. LIGHTFOOT. I certainly don't want you to say anything here that you shouldn't, because we don't want to be a party to giving them anything we don't want them to have. One final question:

You mentioned in your testimony some of the things that motivated people to be spies and what have you. I think there is an acronym within the business: Malice, money, ideology, ego, and I forget what the fourth one is that motivates people.

We are talking about, I guess, changing information here. What about the disinformation side of it? The Soviets, I assume, are

active in that phase of it as well. What seems to motivate people toward this type of thing? I mean those are motivations that we have had for years.

Have you got any clues, something that may be in the screening process, like you mentioned you had the all-American boy, everything looked fine on the surface. What was the thing that made that individual tick, that that Soviet agent apparently got to and flipped that lever?

Mr. PARKER. I really—it is a very difficult question to even come close to answering, because there are so many factors involved. Greed, malice, revenge, any one of those are there, adventure, the idea of being able to get involved in something that is really exotic, and then wind up being carried along in something that they can't control.

I just cannot give you an answer, Mr. Congressman.

Mr. LIGHTFOOT. This may be very difficult to answer, but it goes along that same line, where maybe they first get someone in like you say, a spirit of adventure, what have you, and in essence, they are compromised where they have to stay in the process.

Have you got any idea how many people may be innocently working for the Soviet bloc in terms of disinformation, maybe not necessarily stealing secrets, so to speak, agents of influence and this type of thing, that they may not even realize that they are actually working for or helping them?

Mr. PARKER. I would prefer not to go into that at this time.

Mr. LIGHTFOOT. Thank you. I appreciate that. Thank you, Mr. Chairman.

Mr. ENGLISH. Mr. Neal?

Mr. NEAL. You mentioned in your testimony a number of cases that you had broken, Harper, Cavanagh, Michelson, Horton, and some others. Is there anything common to those successes that we might learn from? Maybe we can take the other side of it first.

Were those people who had had drug, alcohol, financial problems, or was there something else?

Mr. PARKER. Well, in the *Harper* case, if that company had followed its own security procedures, he would not have been able to get into that building on weekends or nights, and xerox the documents that he did.

The *Horton* case, that is so unusual. Again, were there some compromises in following the normal security procedures? The *Michelson* case was a result of a double agent operation that we conducted with the Army.

The Soviets felt they had recruited this individual because, one, he had desire for money, plus he had access, and they believed he was capable of removing documents from his work area.

I think if anything in looking at all of those, it would be a matter of following the appropriate security procedures that are already set down.

Cavanagh should not have been able to walk out of his office with classified documents. There has to be some degree, some additional security within those organizations.

Mr. NEAL. The private organizations you are talking about?

Mr. PARKER. Private facilities, contractor facilities.

Mr. NEAL. Was there something common in the way you were successful in detecting and arresting these people? Was it by focusing on the people that they delivered their information to?

I had the same thought as the chairman. It seems to me he was really on to something when he talked about focusing on the people that receive it rather than the millions of people that we have working in Government.

Mr. PARKER. I think that is certainly a good point, one that we do focus on the hostile presence. We have no desire nor any intention of looking at the American citizens who are carrying out their normal day-to-day responsibilities, which involve classified material.

We are not going to look at them. What we are going to look at are those hostile service officers who are in the United States and who are out making contacts with people.

Mr. NEAL. Were you successful in these cases, *Harper*, *Cavanagh* and all these that you listed? Was there something common in your success? Was it because you were watching the people that received the information?

Mr. PARKER. Yes, because of our ongoing investigations against those services.

Mr. NEAL. It wasn't because you had investigated them personally and found that they had alcohol or drugs or financial problems?

Mr. PARKER. That is correct.

Mr. NEAL. My son was assigned the book, "The Falcon and the Snowman," for school, and I ended up reading it, because he had it around the house there. Are you familiar with that case?

It sounds very much like the way you describe these. Here was a young guy seeking adventure who was working in a place that had very lax security, a defense contractor on the west coast that didn't—

Mr. PARKER. I have not read the book. I am certainly familiar with the case.

Mr. NEAL. You haven't missed a heck of a lot, I will tell you. Anyway, the idea was that this guy, of course, in that story, drugs, alcohol, adventure, money were all involved, but it couldn't have happened unless the security precautions at that defense contractor were lax.

I was asking the other witnesses if they thought we were sort of on the right track. I was asking that question in the context of doing all these background checks and rechecks and so on, on our own people.

I guess my own impression now is that probably if that is what we were depending on, we would be on the wrong track, and we would be more on the right track if we were focusing on where the information would be desired, which would be these agents of hostile powers.

Mr. PARKER. It is certainly not either/or. We have only one facet of the overall protection of our national security. It involves many other agencies, and if any one of those fails, we could have serious problems.

It is not only in the United States. It also involves overseas. The fact that a person says he is who he is may not be true. There are

such individuals who come to the United States and assume the identities of other people.

We have to go through the background investigation to insure that that person is that person. There are at least three areas that I see, counterintelligence, the background check and the physical security, *per se*.

Mr. NEAL. I have missed it in reading the press accounts of the *Walker* case. How was he uncovered?

Mr. PARKER. I am sorry, Mr. Congressman, I can't talk about the case at all.

Mr. NEAL. That is right. I am reminded that his wife mentioned that he was involved in this or something. The chairman already asked this question about a profile. You say there wasn't a profile, but you also indicated that there are certain things that you do, there are threads that you run through this, greed, malice, revenge, I think are the areas that you mentioned?

Mr. PARKER. Yes.

Mr. NEAL. But not enough there where you would feel that that is something that could be picked up?

Mr. PARKER. No. I think you mentioned earlier that there are people who are fired and want to do something against the person who fired them. There are people who have alcohol problems.

There are financial problems, but where does it end that the end result is committing espionage? Everyone has those feelings, or most of us have feelings at one time or another, but we don't take them to the extent that it reaches that serious a threat.

Mr. NEAL. Thank you.

Mr. ENGLISH. Mr. Miller?

Mr. MILLER. With the recent focus on this issue, two of the remedies that have been discussed in recent days, among others, are more use of polygraph tests in the investigation process and more severe sentences of those convicted of espionage, including possible mandatory life sentences, or a death penalty.

Does the FBI have a position on either of these issues?

Mr. PARKER. I am not authorized to state any position on either one at this point. I will say that we use the polygraph as an investigative tool. We find it an extremely valuable tool, but it is not used solely by the FBI nor, I am sure, by any other agency.

Mr. NEAL. Will the gentleman yield on that point?

Mr. MILLER. Yes.

Mr. NEAL. I had asked some questions earlier about the polygraph. Are you at all worried about the problems raised in the hearing I mentioned earlier concerning what I think they characterized as false positives and false negatives? That is, this testimony suggested that the lie detector test, polygraph tests, were no more accurate than a flip of the coin; that there were people who could successfully take the test when lying; that if you indicated those people who were telling the truth who simply became emotionally agitated, that would register on the test, and would give an indication that they were lying when they were not; I think the conclusion of the hearing was that reliance on those tests would give or could give a false confidence.

That is, you would be believing people who were skillful liars, and on the other hand, you would be not believing people in significant numbers who would be telling the truth.

Would you say that testimony is inaccurate, or if it is accurate, why do you rely on it?

Mr. PARKER. I certainly am not a polygrapher nor a polygraph expert. Our experience with the polygraph has been very good. However, it is not the end of any investigation nor do we take a positive or negative polygraph examination as the end to all ends.

Any information, if it is negative or positive, will have to be corroborated before we would take any action, from the results of the use of a polygraph. Insofar as the other testimony, I just could not comment on that.

Mr. NEAL. When you say that it is good, you mean that it helps point you in a direction?

Mr. PARKER. Yes. It has provided us with investigative leads, and with assistance in interviews.

Mr. NEAL. But if you can't rely on it—I have got someone else's time, and I don't want to pursue it.

Mr. PARKER. No; as I say, our experience has been very good with polygraph, insofar as reliability is concerned.

Mr. NEAL. How do you know?

Mr. PARKER. Through the corroboration of the positive or negative results of that investigation, we have been able to corroborate that information.

Mr. NEAL. Thank you.

Mr. MILLER. Thank you.

Mr. ENGLISH. Mr. Spratt, could I ask one quick question that I meant to ask a while ago?

I suppose one thing that is troubling a lot of people, and I have got to say it is sure troubling me, is not the fact that we have had somebody who has been spying. We all recognize that you are going to have a few bad apples in the barrel. There is no question about that.

The real question is how in the world somebody could go for 20 years without getting caught. Does that embarrass the FBI, that somebody could operate for that long and not be identified, that he could be carrying on for that long? I am not presuming anyone's guilt at this point, but just that an agent could operate for that long, evidently carry on a network for that long possibly, without being detected?

Mr. PARKER. For the most part, when a counterintelligence organization brings a case to trial, it indicates a degree of failure, unless in a case such as the Alice Michelson case, where it was a thought-out operation to bring a person to trial.

The Alfred Zaia case, a double-agent operation, to bring a person into the United States for arrest. Those operations have a specific purpose of an arrest.

Other cases, yes, we are disturbed that we have to arrest a U.S. citizen. We would much prefer to prevent espionage than to catch and prosecute.

Mr. ENGLISH. But should it be proven that an agent operated for 20 years, wouldn't that be a particular embarrassment, that somebody could get away with it for that long, and not be detected?

I can understand over a short period of time. It is always an embarrassment to find out that you failed to do your job, but 20 years is a heck of a long time for a fellow to get away with it.

Mr. PARKER. I think you have to look at, when we talked earlier, the points of contact, if these contacts take place outside the United States, there is certainly a problem there that we, in the FBI, are not going to be able to handle alone.

Mr. ENGLISH. Thank you. Mr. Spratt, do you have some questions?

Mr. SPRATT. Mr. Chairman, I don't have any questions for open session. You took one of my questions.

Mr. ENGLISH. I am sorry about that.

Mr. SPRATT. I have read the statement of Mr. Britt Snider, who is an upcoming witness. I thought somewhere in Mr. Snider's statement, it was stated that for a substantial period of time, I believe in the seventies, there were no espionage cases at all. Maybe it was another witness who made that statement. It is not in your statement.

Mr. PARKER. That is not correct.

Mr. SPRATT. A span of several years, 1965 to 1975, there were no espionage cases prosecuted or detected at all. Surely, we can't infer from that that there was no espionage going on during that period.

Mr. PARKER. In 1965, we arrested Robert Glenn Thompson, U.S. Air Force, convicted, sentenced to 30 years. James Alan Mitkenbaugh, Army enlisted man, arrested for conspiracy to commit espionage, 25 years in prison. Robert Lee Johnson, the same time, 25 years, in 1966, William Henry Whelan and Robert Bokenhaup, both convicted of espionage conspiracy in 1966.

In 1973, James David Wood was arrested for conspiracy to commit espionage. In 1975 and 1976, we arrested Sarkis Pascalian and Sahag Dedeyan.

Mr. SPRATT. Apparently, the information was derived from a statement made by Mr. Trott, the Assistant U.S. Attorney General, who indicated that during this period of time, there were no espionage cases prosecuted.

Perhaps some of these were court-martialed and maybe that is what he was talking about.

Mr. PARKER. No. These were—not all——

Mr. SPRATT. U.S. district court.

Mr. PARKER. Yes, sir.

Mr. SPRATT. Do you know why he made that statement?

Mr. PARKER. No, sir.

Mr. SPRATT. Thank you very much. We can ask you that question in closed session. That is all.

Mr. ENGLISH. I have one last question for you. Do you feel that the FBI is doing a good job on counterespionage?

Mr. PARKER. Mr. Chairman, I think the FBI is the best counterintelligence organization in the world. I think we have the manpower, the training, the dedication within our special agent and support personnel to carry out our mandate in an outstanding manner.

We have asked and are receiving additional manpower and support assistance from the Congress, and I think, as time goes by, we

will be even in a greater position to carry out those duties that we have, but yes, sir, I believe we are doing an excellent job.

Mr. ENGLISH. Then, am I to infer from your answer that you feel the FBI has sufficient resources available today to do the job as it sees it today and in the foreseeable future, in carrying out the counterespionage responsibilities?

Mr. PARKER. With the additional resources that you have given us, and that we will be receiving, yes, sir.

Mr. ENGLISH. Even with the fact that—

Mr. PARKER. Today, no; I am looking forward to those additional resources which we will be getting.

Mr. ENGLISH. And that will be sufficient to handle 4,000 Soviet nationals and Eastern bloc citizens that are in this country, regardless of what percentage of those are espionage agents?

Mr. PARKER. Not with all of those additional.

Mr. ENGLISH. But that is the requirement you have today, isn't it?

Mr. PARKER. I think if we can keep the number of hostile service officers at least at the level that they are today, and with the additional benefits that we have received from the Office of Foreign Missions, Foreign Intelligence Surveillance Act, I think by the time we have reached the point that we have been seeking in our resources, we will be able to do our job, yes, sir.

Mr. ENGLISH. In other words, you are not there today?

Mr. PARKER. Not there today.

Mr. ENGLISH. OK. Any further questions?

Mr. LIGHTFOOT. Mr. Chairman, just a quick followup. On your comment, Mr. Parker, and in the last paragraph of your testimony, I think you really hit on something important, if I can quote you, that you were saying that "countermeasures and counter-espionage are relatively easy problems to solve in a totalitarian state. This is not a totalitarian state." I think you gentlemen are charged with an extremely important duty. And I think you do it extremely well in staying within those parameters of the free country that we have.

Are we in any way somewhat tying your hands or do you feel that you can operate as freely as you should with these surveillance types of things that you have to do?

Mr. PARKER. I think, if I might preface the whole thing, we cannot carry out even a small percentage of our job if we don't have the complete cooperation of the American people. And we find that we do have the complete cooperation of the American people. It is a very very small percentage of those who refuse to talk to us.

It is a very very small percentage who are involved in espionage. So we see no roadblocks or straitjackets which prevent us from carrying out our duties as long as we can continue to have the trust of the American people.

Mr. LIGHTFOOT. Keep it up. We need you.

Mr. PARKER. Thank you.

Mr. ENGLISH. We may have some additional written questions for you, Mr. Parker, that we will submit to you. We appreciate your testimony before us today. We will be looking forward to seeing you or one of the other FBI members in closed session. We will try to

get deeper into some of the measures that you take as well as some of the problems that you may be running in. Thank you very much for your testimony today.

Mr. PARKER. Thank you, Mr. Chairman: I enjoyed it very much.

Mr. ENGLISH. Our next witness is Mr. L. Britt Snider, who is Director of the Office of Counterintelligence and Security Policy with the Department of Defense. Mr. Snider, if you would come forward, please, and identify the gentlemen who are accompanying you.

STATEMENT OF L. BRITT SNIDER, DIRECTOR, OFFICE OF COUNTERINTELLIGENCE AND SECURITY POLICY, DEPARTMENT OF DEFENSE, ACCOMPANIED BY JACK DONNELLY, DIRECTOR, COUNTERINTELLIGENCE AND INVESTIGATIVE PROGRAMS, AND MAYNARD ANDERSON, DIRECTOR, SECURITY PLANS AND PROGRAMS

Mr. SNIDER. To my left is Jack Donnelly who is Director for Counterintelligence Investigative Programs in our office. To my right is Mr. Maynard Anderson, Director for Security Plans and Programs in our office.

Mr. ENGLISH. As I have told our other witnesses, if you would like to summarize your testimony, without objection your complete written testimony will be made part of the record.

Mr. SNIDER. Thank you, Mr. Chairman. Since Mr. Thurman, in fact, covered the substance of the earlier part of my statement, I am going to skip toward the end of it in the interest of time.

Mr. Thurman, in fact, covered pretty accurately the size of the problems and what DOD does about it.

At the end of my statement, I speak to what we can do to improve our posture and this is what I would like to confine my remarks to.

Unfortunately, despite all the precautions we take, we have people who decide to commit espionage and manage to escape detection for some period of time. What can be done to prevent this? Ultimately, there is no foolproof way to keep someone from becoming a spy if he chooses to do so. And, although we hope that the measures we have in place will sooner or later detect them, there is not a way to guarantee it.

There are obviously things that might be done to reduce the exposure of classified information in general. Reducing the numbers of people with clearances, as the Secretary has already directed, is one such action. And we are pursuing the goal of further reductions. Obviously, the object is to accomplish the defense mission with as few cleared people as necessary.

Bringing a greater degree of discipline to the classification system is another. We are exploring additional ways to reduce the numbers of classified documents being created—particularly in the higher classification categories—to those absolutely necessary to mission accomplishment.

We are also looking at ways to improve the investigations done on those who require clearances, including, as I mentioned, a limited use of the polygraph where our most sensitive information is involved. The Department has also discussed with Congress the need for statutory authority for our investigators doing background in-

vestigations to obtain criminal history data from State and local jurisdictions where such access is presently denied them. We hope such legislation can be enacted.

There is also undoubtedly more that could be done to improve the odds that espionage will be detected. An increased awareness on the part of supervisors and fellow employees to indicators of espionage would, in my view, produce particular dividends. Perhaps, if nothing else, the Walker case and what we know of it to date, will demonstrate to our employees that no office or activity is immune from the threat.

The resources devoted to the counterintelligence efforts of the Government also clearly impact the problem. These resources have increased substantially in recent years, and at the same time we have been catching more people who are involved, or attempting to become involved, in espionage. Still, the assignment of the U.S. counterintelligence community to keep track of the activities of known or suspected intelligence operatives within the United States is a formidable one.

Not only are resources important in this regard, but the legal confines in which hostile intelligence agents must carry out their activities within the United States are an equally important part of the equation. That environment became more restrictive in recent years, and proposals such as that which passed the Senate several days ago, to reduce the disparity in the number of persons with diplomatic immunity assigned to the Soviet diplomatic establishments in the United States, as opposed to the number assigned our Embassy in Moscow, will help.

Similarly, the proposal made recently by Senator Roth to subject U.N. Secretariat employees from certain countries to many of the same controls that now bind the diplomatic personnel from those countries, will, if enacted, directly benefit the U.S. counterintelligence effort.

But even with these improvements, and even with a great expansion of resources at every level of the U.S. counterintelligence and security structure, we nonetheless must face the ultimate reality that no matter what we do, there will be other espionage cases in the years to come—perhaps not as many; perhaps not as serious. Hopefully, not as drawn out as those which have recently come to light, but there will be other cases. It is the challenge for all of us involved in this area to minimize their occurrence within the limits of our resources and consistent with the values and principles of a free society.

I'll be glad to answer any questions you may have.

[The prepared statement of Mr. Snider follows:]

BEST COPY AVAILABLE

STATEMENT
OF

L. BRITT SNIDER
PRINCIPAL DIRECTOR, COUNTERINTELLIGENCE AND SECURITY POLICY
OFFICE OF THE SECRETARY OF DEFENSE
DEPARTMENT OF DEFENSE

BEFORE

THE SUBCOMMITTEE ON GOVERNMENT INFORMATION, JUSTICE AND AGRICULTURE
COMMITTEE ON GOVERNMENT OPERATIONS
U.S. HOUSE OF REPRESENTATIVES

JUNE 17, 1985

BEST COPY AVAILABLE

MR. CHAIRMAN, IT IS A PLEASURE TO APPEAR BEFORE THIS SUBCOMMITTEE THIS AFTERNOON. I HAVE BEEN ASKED TO DESCRIBE THE PROGRAMS THE DEFENSE DEPARTMENT HAS ONGOING TO PREVENT AND DETECT HOSTILE INTELLIGENCE ACTIVITIES UNDERTAKEN AGAINST OUR EMPLOYEES AND CONTRACTORS, OF THE KIND THAT HAVE RECENTLY COME TO LIGHT IN THE WALKER CASE.

I MUST SAY AT THE OUTSET THAT I AM NOT PREPARED TO COMMENT ON THE WALKER CASE PER SE IN VIEW OF PENDING CRIMINAL ACTIONS. WITHIN THE LIMITS OF CLASSIFICATION, HOWEVER, I'M PREPARED TO DISCUSS THIS SUBJECT WITH YOU. ACCOMPANYING ME ARE MR. JACK DONNELLY, WHO IS DIRECTOR FOR COUNTERINTELLIGENCE AND INVESTIGATIVE PROGRAMS, AND MR. MAYNARD ANDERSON, WHO IS DIRECTOR FOR SECURITY PLANS AND PROGRAMS, BOTH OF OUR OFFICE. BY WAY OF INTRODUCTION, WE ALL WORK FOR THE UNDER SECRETARY OF DEFENSE FOR POLICY WITHIN THE OFFICE OF THE SECRETARY OF DEFENSE, WHO HAS OVERALL POLICY RESPONSIBILITY FOR THE DEPARTMENT'S COUNTERINTELLIGENCE AND SECURITY PROGRAMS.

LET ME BEGIN BY DESCRIBING IN QUANTITATIVE TERMS THE ENORMITY OF THE SECURITY PROBLEM FACED BY THE DEPARTMENT. AS OF THE FIRST OF APRIL, WE HAD A TOTAL OF 4.3 MILLION PERSONS CLEARED FOR SOME FORM OF ACCESS TO CLASSIFIED INFORMATION. OF THESE, 2.9 MILLION WERE CIVILIAN OR MILITARY EMPLOYEES OF THE DEPARTMENT; AND 1.4 MILLION WERE EMPLOYEES OF THE MORE THAN

BEST COPY AVAILABLE

14,000 DEFENSE CONTRACTORS WITH SOME FORM OF SECURITY CLEARANCE. WHILE BY FAR MOST OF THESE CLEARED PERSONS ARE PHYSICALLY WITHIN THE UNITED STATES, DOD HAS SOME FORM OF OFFICIAL PRESENCE WITHIN 120 COUNTRIES AROUND THE WORLD.

THESE CLEARED PERSONNEL CREATE AND HANDLE AN ESTIMATED 16 MILLION CLASSIFIED DOCUMENTS ANNUALLY, OF VARYING DEGREES OF SENSITIVITY.

DOD PERSONNEL, INSTALLATIONS, AND CONTRACTORS HAVE LONG BEEN TARGETS OF ESPIONAGE EFFORTS AS WELL AS OTHER TYPES OF TECHNICAL COLLECTION EFFORTS UNDERTAKEN BY OUR ADVERSARIES. FOR THE MOST PART, OUR PEOPLE AND OUR CONTRACTORS ARE RATHER EASILY IDENTIFIED BY HOSTILE INTELLIGENCE BOTH IN TERMS OF WHERE THEY WORK AND THE SORTS OF ACTIVITIES IN WHICH THEY ARE LIKELY TO BE ENGAGED. WE RECEIVE IN THE NEIGHBORHOOD OF 600 REPORTS ANNUALLY OF POSSIBLE CONTACTS OF HOSTILE INTELLIGENCE SERVICES WITH DOD PERSONNEL. ALL, I MIGHT ADD, ARE REVIEWED AND INVESTIGATED AS APPROPRIATE.

UNFORTUNATELY, WE MUST ALSO RECOGNIZE THAT NOT ALL ESPIONAGE IS INSTIGATED BY THE OTHER SIDE. WE HAVE OCCASIONAL INSTANCES WHERE DEFENSE DEPARTMENT EMPLOYEES AND CONTRACTORS INITIATE THE CONTACTS THEMSELVES, OFFERING TO SELL CLASSIFIED INFORMATION TO WHICH THEY HAVE ACCESS. WHEN WEIGHED AGAINST THE VAST NUMBERS OF CLEARED PEOPLE, HOWEVER, THE NUMBER WHO AGREE TO

BEST COPY AVAILABLE

PARTICIPATE IN, OR INITIATE, ESPIONAGE ACTIVITIES IS INFINITESIMALLY SMALL. BUT IT IS EQUALLY TRUE THAT ONE PERSON WITH THE RIGHT ACCESS MAY BE CAPABLE OF COMPROMISING MILITARY SYSTEMS THAT COST THE U.S. LITERALLY MILLIONS, IF NOT BILLIONS, OF DOLLARS TO DEVELOP AND PRODUCE. THIS MAY LEAD TO ACTIONS TO COUNTER THE LATEST U.S. MILITARY HARDWARE OR THE LATEST U.S. STRATEGY. AND SO, FROM OUR STANDPOINT, EVEN ONE CASE IS TOO MANY;

SO, WHAT DO WE DO TO PREVENT AND DETECT THESE EFFORTS? THERE ARE DEFENSE DIRECTIVES AND REGULATIONS WHICH ADDRESS THIS SUBJECT THAT WOULD LITERALLY REACH FROM THE FLOOR TO THE CEILING OF THIS HEARING ROOM. THEY COVER VIRTUALLY EVERY ASPECT ONE CAN IMAGINE TO PROTECT CLASSIFIED INFORMATION FROM UNAUTHORIZED DISCLOSURE; WITHOUT ATTEMPTING TO DESCRIBE THEM IN DETAIL, LET ME IDENTIFY CONCEPTUALLY THE SORTS OF PROGRAMS ENCOMPASSED HERE.

FIRST, THERE ARE POLICIES GOVERNING THE CLASSIFICATION OF INFORMATION IN THE INTERESTS OF NATIONAL SECURITY. THESE ARE SET FORTH IN EXECUTIVE ORDER 12356 WHICH APPLIES TO ALL DEPARTMENTS AND AGENCIES OF THE EXECUTIVE BRANCH, AS WELL AS ITS CONTRACTORS. FLOWING FROM THIS BASIC DOCUMENT ARE RULES WHICH APPLY TO THE MARKING, HANDLING, REPRODUCTION, ACCOUNTABILITY, TRANSMISSION, STORAGE, AND DESTRUCTION OF SUCH INFORMATION. THESE POLICIES ENCOMPASS NOT ONLY REQUIREMENTS TO LOCK CLASSIFIED INFORMATION IN SAFES, AS ONE MIGHT EXPECT,

BEST COPY AVAILABLE

THEY ALSO COVER SUCH THINGS AS THE KINDS OF TELEPHONES THAT ONE MIGHT USE TO DISCUSS CLASSIFIED INFORMATION; HOW ELECTRONIC EQUIPMENT PROCESSING CLASSIFIED INFORMATION MUST BE SHIELDED TO PREVENT EMANATIONS LEAVING THE AREA; WHAT METHODS ARE ACCEPTABLE FOR DESTROYING CLASSIFIED INFORMATION; HOW INFORMATION TO BE RELEASED TO THE PUBLIC MUST BE SCREENED FOR CLASSIFIED INFORMATION; WHOSE PERMISSION MUST YOU HAVE BEFORE YOU CAN CLASSIFY OR REPRODUCE A CLASSIFIED DOCUMENT; WHAT YOU HAVE TO DO BEFORE YOU CAN SHARE CLASSIFIED INFORMATION WITH AN ALLIED GOVERNMENT; WHEN YOU HAVE TO HAVE AREAS SWEPT ELECTRONICALLY TO DETERMINE THE PRESENCE OF LISTENING DEVICES. IN SHORT, VIRTUALLY EVERY CIRCUMSTANCE ONE CAN THINK OF, IN TERMS OF PRECLUDING THE POSSIBLE EXPOSURE OF CLASSIFIED INFORMATION TO UNAUTHORIZED PERSONS, IS TREATED IN THE REGULATIONS OF THE DEPARTMENT.

THE SECOND MAJOR AREA OF POLICY -- APART FROM HOW CLASSIFIED INFORMATION IS IDENTIFIED AND PHYSICALLY PROTECTED -- GOVERNS WHO SHALL HAVE ACCESS TO IT. IN GENERAL, ACCESS CAN BE GRANTED TO SOMEONE WHOM THE DEPARTMENT HAS DETERMINED TO BE TRUSTWORTHY AND HAS GRANTED A SECURITY CLEARANCE, AND HAS A "NEED-TO-KNOW" INFORMATION CLASSIFIED AT A PARTICULAR LEVEL IN CONNECTION WITH HIS EMPLOYMENT WITH DOD, OR HIS PERFORMANCE ON A DOD CONTRACT.

A CLEARANCE IS NORMALLY REQUESTED BY THE EMPLOYING OFFICE OF A DOD COMPONENT, OR BY A CLEARED DEFENSE CONTRACTOR, WHO

MUST CERTIFY THAT THE INDIVIDUAL INVOLVED HAS A NEED TO ACCESS CLASSIFIED INFORMATION AT THE LEVEL OF THE CLEARANCE BEING REQUESTED. THE REQUEST FOR INVESTIGATION GOES TO THE DEFENSE INVESTIGATIVE SERVICE, WHOSE 1555 INVESTIGATORS CARRY OUT ALL BACKGROUND CHECKS FOR THE DEPARTMENT OF DEFENSE.

THE CHECKS PERFORMED IN A PARTICULAR CASE DEPEND UPON THE LEVEL OF CLEARANCE REQUESTED. IN GENERAL, PERSONS RECEIVING A TOP SECRET CLEARANCE, AND THOSE REQUIRING SPECIAL INTELLIGENCE ACCESSES ARE SUBJECTED TO A FULL FIELD INVESTIGATION, WHILE SECRET AND CONFIDENTIAL CLEARANCES ARE BASED UPON A SO-CALLED "NATIONAL AGENCY CHECK", WHICH AMOUNTS TO A CHECK OF PERTINENT FEDERAL AGENCY FILES, INCLUDING THE FBI, FOR INDICATIONS OF DEROGATORY INFORMATION CONCERNING THE SUBJECT.

ONCE THE FIELD INVESTIGATION OR NATIONAL AGENCY CHECK HAS BEEN COMPLETED, THE RESULTS ARE PROVIDED TO THE REQUESTING DOD COMPONENT, OR IN THE CASE OF DEFENSE CONTRACTORS, THE DEFENSE INDUSTRIAL SECURITY CLEARANCE OFFICE, FOR A DECISION WHETHER A CLEARANCE SHOULD BE ISSUED THE INDIVIDUAL.

THE PROCESS DOES NOT END THERE, HOWEVER. SINCE 1983, COMPREHENSIVE REINVESTIGATIONS ARE BEING DONE FOR THOSE WITH TOP SECRET AND SPECIAL INTELLIGENCE ACCESSES. FOR THE LAST TWO YEARS, DIS HAS DONE ROUGHLY 40,000 OF THESE. SUPERVISORS OF CLEARED EMPLOYEES BOTH IN DOD AND IN INDUSTRY ALSO HAVE A

BEST COPY AVAILABLE

CONTINUING RESPONSIBILITY TO IDENTIFY AND REPORT FACTS THAT BECOME KNOWN TO THEM CONCERNING THESE CLEARED EMPLOYEES WHICH MAY HAVE SECURITY SIGNIFICANCE. ALL SUCH REPORTS ARE INVESTIGATED BY DIS OR THE MILITARY SERVICES, AS MAY BE APPROPRIATE.

THERE ARE ALSO REQUIREMENTS IN DOD AND IN DEFENSE INDUSTRY FOR PERIODIC SECURITY AWARENESS BRIEFINGS, WHEN CLEARED EMPLOYEES ARE ADVISED OF THE THREAT POSED BY HOSTILE INTELLIGENCE COLLECTION AND WHAT TO DO SHOULD THEY BE CONTACTED. APPROXIMATELY 1.3 MILLION PERSONS WERE REACHED BY SUCH BRIEFINGS LAST YEAR. THEY WERE SUPPLEMENTED IN DEFENSE INDUSTRY BY FBI BRIEFINGS, AS WELL.

IN ADDITION TO THESE MEASURES WHICH HAVE GENERAL APPLICABILITY TO ALL CLASSIFIED PROGRAMS, WE ALSO HAVE RULES THAT APPLY TO ESPECIALLY SENSITIVE CLASSIFIED INFORMATION PROTECTED WITHIN SO-CALLED "SPECIAL ACCESS PROGRAMS". EXECUTIVE ORDER 12356 AUTHORIZES THE SECRETARY OF DEFENSE AND THE SECRETARIES OF THE MILITARY DEPARTMENTS TO CREATE SPECIAL SECURITY COMPARTMENTS TO PROTECT UNUSUALLY SENSITIVE CLASSIFIED INFORMATION. AT A MINIMUM, ONLY PERSONS WHO HAVE BEEN SPECIFICALLY DESIGNATED FOR THE PARTICULAR INFORMATION ARE ELIGIBLE FOR ACCESS. IN ESSENCE, THE SPECIAL ACCESS PROGRAM IS A WAY OF INSTITUTIONALIZING THE "NEED-TO-KNOW" PRINCIPLE. ADDITIONAL SECURITY MEASURES NOT OTHERWISE REQUIRED WITH RESPECT TO "NORMAL" CLASSIFIED INFORMATION ARE TYPICALLY REQUIRED, TAILORED TO MEET THE PARTICULAR NEEDS OF THE PROGRAM IN QUESTION.

BEST COPY AVAILABLE

I SHOULD ALSO MENTION THAT WITH RESPECT TO THESE SPECIAL ACCESS PROGRAMS THAT DOD IS CURRENTLY IMPLEMENTING A TEST PROGRAM UTILIZING A LIMITED POLYGRAPH EXAMINATION AS A CONDITION OF ACCESS TO SUCH PROGRAMS. AS YOU MAY BE AWARE, CONGRESS AUTHORIZED DOD TO CONDUCT SUCH A TEST OF THE POLYGRAPH -- LIMITED TO 3500 PERSONS -- AS PART OF LAST YEAR'S DEFENSE AUTHORIZATION ACT. AT THE CONCLUSION OF THIS TEST, DOD WILL REPORT ITS RESULTS TO THE CONGRESS AND SUBMIT RECOMMENDATIONS ON A FUTURE PROGRAM.

THE THIRD MAJOR AREA OF POLICY DEALS WITH ENFORCEMENT OF THE RULES. I HAVE ALREADY MENTIONED THE FACT THAT THE SYSTEM ITSELF HAS A BUILT-IN SELF-POLICING ASPECT. ALL SUPERVISORS OF CLEARED PERSONNEL ARE CHARGED WITH THE RESPONSIBILITY FOR IDENTIFYING AND REPORTING INFORMATION OF SECURITY SIGNIFICANCE CONCERNING THEIR EMPLOYEES; SECURITY VIOLATIONS ALSO MAY BE REPORTED ON AN ANONYMOUS BASIS OVER THE DOD HOTLINE, ESTABLISHED AND OPERATED BY THE DOD INSPECTOR GENERAL. REPORTS MADE IN ACCORDANCE WITH BOTH PROCEDURES ARE INVESTIGATED BY THE DEFENSE INVESTIGATIVE SERVICE, OR THE MILITARY SERVICES AS MAY BE APPROPRIATE.

THERE ARE ALSO A VOLUMINOUS NUMBER OF SECURITY INSPECTIONS WHICH PERIODICALLY OCCUR. 26,000 WERE DONE WITHIN DOD IN 1984. IN ADDITION, ALL DEFENSE CONTRACTORS WHO HOLD SECURITY

CLEARANCES ARE PERIODICALLY INSPECTED BY THE DEFENSE INVESTIGATIVE SERVICE TO DETERMINE COMPLIANCE WITH DOD POLICY.

WITH RESPECT TO DETECTING ACTUAL INSTANCES OF ESPIONAGE, EACH OF THE MILITARY DEPARTMENTS HAS A COUNTERINTELLIGENCE INVESTIGATIVE AGENCY RESPONSIBLE FOR THEIR PARTICULAR BRANCH OF SERVICE. IN THE ARMY, THE RESPONSIBILITY RESTS WITH THE ARMY INTELLIGENCE AND SECURITY COMMAND; IN NAVY, WITH THE NAVAL INVESTIGATIVE SERVICE; AND IN THE AIR FORCE, WITH THE AIR FORCE OFFICE OF SPECIAL INVESTIGATIONS. EACH OF THESE AGENCIES CONDUCTS COUNTERINTELLIGENCE INVESTIGATIONS AND OPERATIONS DESIGNED TO DETECT SPIES WITHIN THEIR RANKS. IN THE UNITED STATES, ALL OF THESE ACTIVITIES ARE UNDERTAKEN JOINTLY WITH THE FBI. OVERSEAS, THEY ARE COORDINATED WITH THE CIA. THE SUBCOMMITTEE SHOULD ALSO RECOGNIZE THAT OUR INVESTIGATIVE JURISDICTION IN THESE MATTERS IS LIMITED TO MILITARY PERSONNEL; THE FBI HAS PRIMARY INVESTIGATIVE JURISDICTION OVER ALL DEFENSE DEPARTMENT CIVILIAN PERSONNEL AND CONTRACTORS, AND THEY COORDINATE SUCH ACTIVITIES WITH MY OFFICE.

FINALLY, WE RECEIVE CRITICAL SUPPORT FROM THE FBI, AND, OCCASIONALLY FROM OTHER AGENCIES, IN TERMS OF IDENTIFYING DOD PERSONNEL WHO MAY BE INVOLVED IN ESPIONAGE. IT IS VERY MUCH A COOPERATIVE EFFORT.

UNFORTUNATELY, DESPITE ALL OF THIS, WE HAVE PEOPLE WHO DECIDE TO COMMIT ESPIONAGE AND MANAGE TO ESCAPE DETECTION FOR

BEST COPY AVAILABLE

SOME PERIOD OF TIME. WHAT CAN BE DONE TO PREVENT THIS? ULTIMATELY, THERE IS NO FOOLPROOF WAY TO KEEP SOMEONE FROM BECOMING A SPY IF HE CHOOSES TO DO SO. AND, ALTHOUGH WE HOPE THAT THE MEASURES WE HAVE IN PLACE, WILL SOONER OR LATER DETECT HIM, THERE IS NOT A WAY TO GUARANTEE IT.

THERE ARE OBVIOUSLY THINGS THAT MIGHT BE DONE TO REDUCE THE EXPOSURE OF CLASSIFIED INFORMATION IN GENERAL. REDUCING THE NUMBERS OF PEOPLE WITH CLEARANCES, AS THE SECRETARY HAS ALREADY DIRECTED, IS ONE SUCH ACTION AND WE ARE PURSUING THE GOAL OF FURTHER REDUCTIONS. OBVIOUSLY, THE OBJECT IS TO ACCOMPLISH THE DEFENSE MISSION WITH AS FEW CLEARED PEOPLE AS NECESSARY.

BRINGING A GREATER DEGREE OF DISCIPLINE TO THE CLASSIFICATION SYSTEM IS ANOTHER. WE ARE EXPLORING ADDITIONAL WAYS TO REDUCE THE NUMBERS OF CLASSIFIED DOCUMENTS BEING CREATED - PARTICULARLY IN THE HIGHER CLASSIFICATION CATEGORIES - TO THOSE ABSOLUTELY NECESSARY TO MISSION ACCOMPLISHMENT.

WE ARE ALSO LOOKING AT WAYS TO IMPROVE THE INVESTIGATIONS DONE ON THOSE WHO REQUIRE CLEARANCES, INCLUDING, AS I MENTIONED, A LIMITED USE OF THE POLYGRAPH WHERE OUR MOST SENSITIVE INFORMATION IS INVOLVED. THE DEPARTMENT HAS ALSO DISCUSSED WITH CONGRESS THE NEED FOR STATUTORY AUTHORITY FOR OUR INVESTIGATORS DOING BACKGROUND INVESTIGATIONS TO OBTAIN CRIMINAL HISTORY DATA FROM STATE AND LOCAL JURISDICTIONS WHERE SUCH ACCESS IS PRESENTLY DENIED THEM. WE HOPE SUCH LEGISLATION CAN BE ENACTED;

BEST COPY AVAILABLE

THERE IS ALSO UNDOUBTEDLY MORE THAT COULD BE DONE TO IMPROVE THE ODDS THAT ESPIONAGE WILL BE DETECTED. AN INCREASED AWARENESS ON THE PART OF SUPERVISORS AND FELLOW EMPLOYEES TO INDICATORS OF ESPIONAGE WOULD, IN MY VIEW, PRODUCE PARTICULAR DIVIDENDS. PERHAPS, IF NOTHING ELSE, THE WALKER CASE AND WHAT WE KNOW OF IT TO DATE, WILL DEMONSTRATE TO OUR EMPLOYEES THAT NO OFFICE OR NO ACTIVITY IS IMMUNE FROM THE THREAT.

THE RESOURCES DEVOTED TO THE COUNTERINTELLIGENCE EFFORTS OF THE GOVERNMENT ALSO CLEARLY IMPACT THE PROBLEM. THESE RESOURCES HAVE INCREASED SUBSTANTIALLY IN RECENT YEARS, AND AT THE SAME TIME WE HAVE BEEN CATCHING MORE PEOPLE WHO ARE INVOLVED, OR ATTEMPTING TO BECOME INVOLVED, IN ESPIONAGE. STILL, THE ASSIGNMENT OF THE U.S. COUNTERINTELLIGENCE COMMUNITY TO KEEP TRACK OF THE ACTIVITIES OF KNOWN OR SUSPECTED INTELLIGENCE OPERATIVES WITHIN THE U.S. IS A FORMIDABLE ONE. NOT ONLY ARE RESOURCES IMPORTANT IN THIS REGARD, BUT THE LEGAL CONFINES IN WHICH HOSTILE INTELLIGENCE AGENTS MUST CARRY OUT THEIR ACTIVITIES WITHIN THE U.S. ARE AN EQUALLY IMPORTANT PART OF THE EQUATION. THAT ENVIRONMENT BECAME MORE RESTRICTIVE IN RECENT YEARS, AND PROPOSALS SUCH AS THAT WHICH PASSED THE SENATE SEVERAL DAYS AGO, TO REDUCE THE DISPARITY IN THE NUMBER OF PERSONS WITH DIPLOMATIC IMMUNITY ASSIGNED TO THE SOVIET DIPLOMATIC ESTABLISHMENTS IN THE U.S., AS OPPOSED TO THE NUMBER ASSIGNED OUR EMBASSY IN MOSCOW, WILL HELP. SIMILARLY, THE

BEST COPY AVAILABLE

PROPOSAL MADE RECENTLY BY SENATOR ROTH TO SUBJECT UN SECRETARIAT EMPLOYEES FROM CERTAIN COUNTRIES TO MANY OF THE SAME CONTROLS THAT NOW BIND THE DIPLOMATIC PERSONNEL FROM THOSE COUNTRIES, WILL, IF ENACTED, DIRECTLY BENEFIT THE U.S. COUNTERINTELLIGENCE EFFORT.

BUT EVEN WITH THESE IMPROVEMENTS, AND EVEN WITH A GREAT EXPANSION OF RESOURCES AT EVERY LEVEL OF THE U.S. COUNTERINTELLIGENCE AND SECURITY STRUCTURE, WE NONETHELESS MUST FACE THE ULTIMATE REALITY THAT NO MATTER WHAT WE DO THERE WILL BE OTHER ESPIONAGE CASES IN THE YEARS TO COME - PERHAPS NOT AS MANY; PERHAPS NOT AS SERIOUS; HOPEFULLY NOT AS DRAWN OUT, AS THOSE WHICH HAVE RECENTLY COME TO LIGHT, BUT THERE WILL BE OTHER CASES. IT IS THE CHALLENGE FOR ALL OF US INVOLVED IN THIS AREA TO MINIMIZE THEIR OCCURRENCE WITHIN THE LIMITS OF OUR RESOURCES AND CONSISTENT WITH THE VALUES AND PRINCIPLES OF A FREE SOCIETY.

I'LL BE GLAD TO ANSWER ANY QUESTIONS YOU MAY HAVE.

BEST COPY AVAILABLE

Mr. ENGLISH. Thank you very much, Mr. Snider. You didn't mention one of the proposals that I made. I would like to get your thoughts on that.

Mr. SNIDER. Please.

Mr. ENGLISH. I suppose it could be identified as a use-it-or-lose-it-type clearance. If the person doesn't use his security clearance over a given period of time; he would automatically lose it. That would eliminate the need for a person to be reinvestigated.

I would think it would cut down substantially on that. I think that would be particularly true of those persons who have a top secret clearance for which reinvestigation is definitely needed. Do you have any views with regard to that type of proposal?

Mr. SNIDER. Generally, I would agree with it. First of all, we have something to that effect in Defense now. In the industrial area, for example, any firm who has a clearance who completes work on a classified contract has to return the classified documents that it had been given as part of that contract with the department.

Its clearance status then becomes dormant for a period of 9 months. If it gets no additional classified defense work, it loses its security clearance. So there is a sort of a sunset feature built into the program.

Mr. ENGLISH. That would not apply to individuals, though, would it?

Mr. SNIDER. Yes, anyone employed by the company.

Mr. ENGLISH. To any individual?

Mr. SNIDER. Anyone who is employed by the company would also lose his clearance. We have a similar situation in the military departments and defense components. If you are in a particular job with, say, a top secret clearance, and you are then moved to another position that does not require such a clearance, in most cases your clearance level would be automatically decreased to the level that is required for your performance in a particular position.

The only significant exception I know to that is the Air Force where I believe once its personnel are cleared at whatever level, they carry that clearance throughout their military service.

Mr. ENGLISH. It is my understanding, Mr. Snider, that the business of a person moving from one place to the next and having his security clearance downgraded has not been a matter of practice in the past, has it? Routinely, has this been taking place?

Mr. SNIDER. Routinely, downgrading does take place. This is with the exception of Air Force. You are debriefed when you leave a particular position, and then you are reinstated in your new position with whatever clearance is required.

Mr. ENGLISH. Then as I understand it, you would look favorably upon a proposal that if a person, does not need that clearance over a given period of time, say, 3 or 4 years or maybe even less, he or she would automatically lose that clearance, is that correct?

Mr. SNIDER. I would agree with you, in fact, Mr. Chairman. The Secretary's decision to reduce the number of clearances is in fact directed at this target. People who have clearances, but who do not require access to classified information, that is the group that we are looking at first in order to get them out of the system.

Mr. ENGLISH. Part of the testimony we heard earlier dealt with classified material, and in fact, I was asking Mr. Thurman if it would appear that the greater the proliferation of classified material, then the greater the need for people to have security clearances. And he has determined and reported to us that DOD contractors, as well as the Defense Department itself, has a good deal of overclassification taking place. A lot of this would lead to more clearances being requested than would be necessary.

Has DOD got any kind of plan to address this overclassification issue?

Mr. SNIDER. Yes, sir, we have, of course, under our existing policies a requirement that any employee who thinks that a document is overclassified is supposed to raise this with the originator of the document. That is already written into the policy, if you will, and we make inspections every year to determine whether people are carrying out these instructions correctly.

There is a problem. Don't misunderstand. I think there is some overclassification in DOD, no doubt about it. How large a problem it is, the magnitude of it, I don't think anyone really knows. I see thousands of classified documents every year cross my desk. I would say perhaps 2 or less percent I would judge were overclassified. And I go back in every case to the person that classified it and ask him to explain it. That is what the rules are. That is what the policies are.

Mr. ENGLISH. Well, I recognize that, but I think given what GAO found in both 1981 and 1979, you have got a significant problem of overclassification. Here we have the defense contractors. In 1981, of the sample, they were running 51 percent of the documents being overclassified. You have—that was the contractors, and DOD itself in 1979, you had 24 percent. This brings on the need for additional classification. And we even have, back in 1981, July, Ed Meese the Attorney General, stating that he thinks there is way too much classification taking place.

All of this would seem to lead to all kinds of difficulty for people who are in counterintelligence, and for our own security system. It gets back to the same thing of cheapening the security classification itself. I would say that it would likely cheapen the clearance. A top secret clearance won't mean as much as it would otherwise.

Mr. SNIDER. We couldn't agree more with your observation there. Obviously, it is a problem for us in protecting information if we classify it. It costs us, in terms of administrative costs, overhead costs. You are quite right that I think it breeds a disrespect for the system and leads to compounded abuses. We will do everything we can to correct it. It is a tough problem, however, because an element of judgment is involved in classifying a document.

Mr. ENGLISH. Do we have people today, Mr. Snider, who are requesting clearances as something of a status symbol or a way of getting a promotion at a job? Is there some of that taking place as far as requests for security clearance?

Mr. SNIDER. Again, I am quite sure there is some of that. How much it is difficult to quantify. We have a particular problem in industry. Whoever wants to compete for classified defense contracts must be cleared and the number of classified employees that that firm has in terms of bidding on those contracts puts them in a

better competitive position for those contracts. There is built in incentive for industry at least to get as many people cleared as you can.

Mr. ENGLISH. There are, as I understand it, special access contracts that are being used for compartmentalization of the contractor. We also have had some reports that this is a means of keeping people elsewhere in the Pentagon from knowing what this particular section is doing. The information may not be that classified; it may not be anything that they shouldn't know about. If you have some reason you don't want them to find out, you designate with the special classification.

Is that taking place, as well?

Mr. SNIDER. I am not aware that special access programs are being created to avoid the normal oversight and audit process that goes on with respect to DOD contracts. I don't think that is the case. But there are a lot of special access programs being created particularly to protect the sophisticated technology involved in defense contracting.

Mr. ENGLISH. We have a 1983 General Accounting Office report that was prepared for us on special access programs, in which GAO says that it did find that special access contracts are being used for reasons other than the protection of sensitive information.

Mr. SNIDER. I read that report, Mr. Chairman, and we went to GAO after it was published and asked them to identify those contractors for us since we were not aware of these allegations ourselves, and they refused to do so. So, we had no way of following up on this information.

Mr. ENGLISH. Did you carry out your own independent investigation to see if this in fact was taking place?

Mr. SNIDER. We are continuously trying to identify this problem where it exists. If we find it exists, we investigate it and we stop it.

Mr. ENGLISH. Wouldn't one of the best ways to deal with the classification problem, and then also the clearance problem at the same time—wouldn't it be to write some tight guidelines as to what a person is supposed to classify and what designation they should classify it, as opposed to having the kind of a loose, general ballpark, you know, when-in-doubt-classify type policy?

Mr. SNIDER. Certainly it would. We have in the Defense Department over 1,400 classification guides which tell everyone involved in a particular program what elements of that program are classified at what level. We try to avoid, to the extent we can, this element of judgment in what classification is assigned.

These classification guidelines are essentially keyed to particular types of hardware, defense equipment, that is classified. We are, in fact, looking at expanding this concept to other types of classified programs that DOD runs other than, particular hardware or systems.

Mr. ENGLISH. This was, of course, again something Mr. Thurman was telling us about. Particularly as far as DOD contractors, whenever they would request information from DOD as to how certain things should be classified, they weren't getting any of these definitive answers as to where they should draw the line.

Is there any work under way in DOD to address that problem?

BEST COPY AVAILABLE

Mr. SNIDER. Yes, sir. Every classified contract that we let, we attach a form to it which sets forth what parts of a contract are classified at what level.

Again, we are attempting to decide for the contractor as part of the contractual process what is about this contract that is classified and what the contractor must do to protect it.

I think the problem is that quite frequently, despite all of that guidance given to a contractor, he doesn't apply it or he doesn't get much help in applying it later on. We hear frequent complaints about that coming from defense contractors.

Mr. ENGLISH. There is no one then in the Department of Defense that is looking over the shoulder and seeing whether they are doing this properly or not; is that correct?

Mr. SNIDER. Mr. Anderson is our expert in the area.

Mr. ANDERSON. Yes, Mr. Chairman, there are. We have an ongoing program of classification management and oversight. There is, for example, a classification management specialist in every region of the Defense Investigative Service who is attempting to provide that kind of guidance to the contractors in his region.

We have, in addition, a classification management specialist at the headquarters to try to do that. They are part of that body that you spoke of earlier, I think, which is too small to do the job they are trying to do at the moment.

Mr. ENGLISH. I see. So what you are telling me, the reason we got all of this overclassification in 1981 with the defense contractors in particular, is that you simply don't have the manpower, the resources to give them the kind of oversight that you would like to have to cut back on that sort of activity; is that correct?

Mr. ANDERSON. There are more now than there were in 1981, but there is still an inadequate number.

Mr. ENGLISH. How many more now than in 1981?

Mr. ANDERSON. I think there probably are twice as many, but that still doesn't amount to a large number of people devoted to classification management.

Mr. ENGLISH. How many is that?

Mr. ANDERSON. I think we are talking, in terms of the overall effort, about 25 people.

Mr. ENGLISH. Twenty-five people?

Mr. ANDERSON. Yes, sir.

Mr. ENGLISH. To overlook the contractors?

Mr. ANDERSON. Yes.

Mr. ENGLISH. 14,000?

Mr. ANDERSON. The classification management aspect.

Mr. ENGLISH. 14,000 firms, 1 million employees, and you have got 14 folks to do the job?

Mr. ANDERSON. These are personnel dedicated solely to classification management, looking at disputes, giving guidance.

Mr. ENGLISH. You don't get around looking over the shoulder very often?

Mr. ANDERSON. Contractors also receive guidance of course, from the industrial security representative, who inspects that contractor. There are 200 or so of those who inspect the contractor facilities. And when they encounter a problem with classification management, it is brought to the attention of the specialist.

Mr. ENGLISH. Well——

Mr. SNIDER. I don't know if Mr. Anderson left you with the impression there are only 25 people working industrial security——

Mr. ENGLISH. I realize——

Mr. SNIDER [continuing]. At each regional office.

Mr. ENGLISH. As far as the overall security management, I believe for industry you have got around 200, 250; isn't that right?

Mr. ANDERSON. Yes, sir.

Mr. ENGLISH. And there are only 25 of those, though, that would be involved in this process of overseeing the actual classification and whether it is being used properly?

Mr. ANDERSON. Aside from two people in our office who look at the classification guides that come in.

Mr. ENGLISH. 14,000 firms—installations, I should say—and 1 million employees. What would you think that it would take in the way of resources to be able to do an adequate job of making certain that we are getting the proper classification? And, at the same time, the proper clearances for those employees?

Mr. ANDERSON. That is a very difficult problem to answer in terms of numbers. I think we must start in some of our programs to reduce classified holdings. One of the ways to do that, of course, is to impose better classification management to enable us to better protect that which is really sensitive.

Also, you have to remember that about 90 or 95 percent of the classified holdings is in the hands of 4 percent of those 14,000 contractors.

Mr. ENGLISH. The installation is where the problem is. You have to have people for those installations. You can't have one at the firm's headquarters.

Mr. ANDERSON. We also need more—I think if we doubled that force of classification management specialists in terms of numbers——

Mr. ENGLISH. You think 450 can do the job?

Mr. ANDERSON. We need to better educate the people who are making those decisions. That is a significant part of the process. I think if we did that there would be improvement—the more you educate, the better product you get and less oversight you need.

Mr. ENGLISH. I guess the problem that I have is that this committee, 2 years ago, started pointing out that we were going to have a problem as far as overclassification. We thought we had one then. We pointed out what the present Attorney General had to say at that time, and we hit it pretty hard. We also had a hearing with regard to the President's new Executive order dealing with security information; and we pointed out that we thought that this is going to lead to more frequent classification.

We pointed out the fact that at that time, under that order, we could have the Department of Defense deciding that every road map in the country ought to be classified simply because it showed the interstate highways and showed the weak points in the highways, namely, the bridges. Under that Executive order you could classify every telephone book because it contained the names of people who had security clearances.

I don't think it is any real puzzle why we have overclassification taking place.

Do you think there is going to be a real attempt to define and draw some lines as to where the boundaries are for classified information? Is there a plan, any work, under way to do that at the present time?

Mr. SNIDER. Yes, sir. We have a number of things that are under consideration internally now at DOD to tighten up the whole process. I will be glad to share them with the subcommittee once they are done, and hope an answer will be taken in the near future. We have made a proposal to the Under Secretary for Policy in this regard.

I might also add that the Commission that the Secretary established to look at DOD security, in lieu of the Walker case, which is going to be chaired by General Stilwell, is also charged to look at the Information Security Program and practices of the Department of Defense, and recommend changes to the Secretary. That internal review will take place in the near future.

Mr. ENGLISH. Is there consideration at the White House, to your knowledge, to redraw that Executive order?

Mr. SNIDER. I have heard nothing along those lines.

Mr. ENGLISH. Would that be helpful? Tightening up and redefining the Executive order?

Mr. SNIDER. I am not sure it really is a problem with the Executive order so much as a problem of implementing the rules that the Executive order and Defense Department set forth. The policy is fairly sound, in my view.

Mr. ENGLISH. Mr. Lightfoot.

Mr. LIGHTFOOT. Thank you, Mr. Chairman.

I would like to read you a quote and see if you agree with this or not:

When you overclassify, you weaken the whole security system. Throughout 180 years of our Government, however, I have never seen a man court-martialed for overclassifying a paper. That is the reason, I am sure, we are in the mess we are in today.

Does that ring true?

Mr. SNIDER. I think it rings true. Again, we are not really sure of the magnitude of this problem.

Mr. LIGHTFOOT. I guess the point I was going to make is, this was in testimony before this subcommittee from Vice Adm. John Hoskins on November 18, 1957, so I guess it is not a new problem.

Mr. SNIDER. It has not changed.

Mr. LIGHTFOOT. Aren't you in DOD kind of caught in a crossfire on this overclassification thing? There was a case—I don't remember all the details—in recent years where one had picked up a technical manual and it had gotten into the hands of the Soviet bloc. It was laying on a shelf. And it turned out that it gave them some of the secrets for one of our intelligence satellites, and so on. And there are those who feel a lot of older technical data may no longer need to be classified, but it still has value to the Soviet bloc.

How do you strike a balance on those kind of things? Where do you make that decision over what should or should not be classified?

Mr. SNIDER. The originator makes a decision in terms of declassification of a particular document. Hopefully, he will be aware of what the Soviets know and don't know about whatever program is

involved, and that is factored into his determination whether to declassify or not. He is, presumably, also aware of what has been made public concerning the subject, and what is within other countries' capabilities, so that those kinds of criteria figure into his decision whether or not to declassify.

Mr. LIGHTFOOT. Earlier in some other testimony and in your written testimony you are talking about supervisors being responsible for identifying and reporting information of security significance concerning an employee. The GAO witnesses testified that agencies sometimes are reluctant to revoke security clearances because it could be considered as an adverse action, and so on.

Do you agree with that statement insofar as DOD is concerned, and would you care to comment on the problems confronting a supervisor if he is put in that position within your agency?

Mr. SNIDER. Yes.

I don't entirely agree with that statement. I think supervisors in DOD, while it does present something of a problem to them, in fact, do report information concerning their employees. And they do it in industry. And we, in fact, have four times more people whose clearances are revoked in DOD because of the information reported by supervisors than there are turned down as a result of initial background investigations.

So that I would take issue with the statement that employers just simply don't do it. It is an important part of the process. And my own view is, if employers and supervisors would report things to us, that is probably going to be our best source in terms of indicators of espionage. They are the people, in fact, who are in contact each day with Defense Department employees, so they are a key part of the process.

Mr. LIGHTFOOT. Referring to your prepared statement on page 9, you mentioned the need for statutory authority for DOD investigators doing background investigations to obtain criminal history data from State and local jurisdictions where such access is presently denied to them. Could you elaborate for us on some of the legal obstacles that you run into in obtaining that kind of information? Maybe you could describe the legislative proposal that you might have in mind that would change that status.

Mr. SNIDER. I would be glad to. A number of States have passed statutes that in fact preclude their law enforcement agencies from providing criminal history records for any other purpose other than law enforcement. Our investigators go to these agencies for the purpose of getting information for security clearance, and they are turned down without really any recourse, notwithstanding the fact that the subject of the investigation has of course consented to our obtaining these records. But State and local agencies are not able to provide it, because they are legally prohibited from doing so.

We have suggested to a number of people, primarily the Nunn subcommittee in the Senate, that held hearings on this recently, a legislative proposal which would in effect require State and local jurisdictions to provide criminal history data to DOD investigators doing background investigations. Otherwise, we run the risk of clearing people who may have committed felonies, for all we know.

Mr. LIGHTFOOT. So you feel like you need a little more——

Mr. SNIDER. We need to know if someone is a felon before we clear him for top secret or special access programs. It seems to me that is minimal in terms of the Government's needs for information on people who are being cleared.

Mr. LIGHTFOOT. Thank you, Mr. Chairman.

Mr. ENGLISH. Thank you very much, Mr. Lightfoot.

According to the GAO, the clearance office received 2,400 reports of adverse information in 1984, and based on these reports, only suspended 24 clearances. That would appear to be—and this was until the investigation could be completed, of course, this was in the interim—that would appear to be questionable.

It would seem to me if you received adverse information, particularly 2,400 pieces of adverse information, which I assume was on a large number of people, certainly far more than 24, that you would suspend, on an interim basis at least, those people until this was either proven or disproven. Can you explain why that was not done?

Mr. SNIDER. Well, I can just generally tell you that we do suspend clearances when there is an immediate threat to the classified information that is indicated by whatever the adverse information is. If we have information that this individual is in unauthorized contact with foreign powers, for example, we may take suspension action in that, wherever we think there is an immediate threat to the information.

If on the other hand it is alleged that he has drinking problems or financial problems, we may not see the immediate threat posed to classified information, to which he may have access, so we don't suspend his clearance. But the investigation that is done on that individual is then reported to the clearing authority, who makes a decision whether, on the basis of his kind of activity, the clearance should be revoked. That is generally what happens.

Mr. ENGLISH. Mr. Snider, we will probably have some additional written questions that we will submit to you, but I think this will be all the questions that we have that we can discuss in public at this time. We appreciate your testimony. Thank you for coming by.

Mr. SNIDER. It is my pleasure. Thank you, sir.

Mr. ENGLISH. Next, we will have a panel including Lanny E. McCullah, Assistant Director for Counterintelligence, Naval Investigative Service; and Robert C. Allen, Director, Security Policy, Office of Naval Operations, U.S. Navy.

Mr. McCullah.

STATEMENT OF LANNY E. McCULLAH, ASSISTANT DIRECTOR FOR COUNTERINTELLIGENCE, NAVAL INVESTIGATIVE SERVICE, U.S. NAVY

Mr. McCULLAH. Mr. Chairman and members of the subcommittee—

Mr. ENGLISH. Would you like to summarize your testimony?

Mr. McCULLAH. I certainly would, in the interests of time. I have submitted a statement for the record.

Mr. ENGLISH. The complete written testimony will be made a part of the record.

Mr. McCULLAH. Thank you.

I would like to state that the current mission in the Naval Investigative Service is threefold: Criminal (felony) investigations, counterintelligence, and physical security law enforcement policy for the Department of the Navy. Today, again in the interests of time, I will just address the counterintelligence aspect of our mission. The Navy Foreign Counterintelligence Program functions in accordance with guidance provided by the Director of Naval Intelligence and the Department of Defense.

The Navy Foreign Counterintelligence Program is executed for the Director of Naval Intelligence by the Director, Naval Investigative Service, exercising worldwide control and direction over the more than 150 offices of the NIS.

Present NIS civilian special agent staffing is 974, with approximately 20 percent dedicated to the FCI arena.

For comparison to our present strength, the total special agent allowance in fiscal year 1981 was only 590, with none dedicated specifically to the specialties of FCI and fraud. In other words, an agent was a generalist who was expected to address the full range of investigative matters. Since then, we have been able to significantly increase the number of dedicated FCI agents through improved funding and long-range planning.

This was facilitated in part by the re-emphasis on counterintelligence contained in Executive Order 12333 and the subsequent support of the Director of Central Intelligence, Deputy Under Secretary of Defense for Policy and the Director of Naval Intelligence.

Starting in fiscal year 1982, identified fenced points were provided to NIS to allow for the dedication of FCI agents to the functional areas of investigations, operations, and collection and production. Our out-year projections call for approximately 500 to 600 FCI dedicated personnel to meet our CI mission requirements and the ever-changing additional responsibilities and priorities. Regardless of all recent resource enhancements, additional future programmed growth is required.

With the advent of FCI dedicated personnel, NIS recognized that a tailored training program was necessary in order to achieve our desired results. All NIS agents enter with at least one college degree, and receive a combination of 11 weeks' intensive basic investigative training and on-the-job training, followed by a general investigative assignment and more on-the-job training before becoming eligible for selection to the FCI program.

At that point, we initiate a cycle of 10 different specialized blocks of FCI training. NIS FCI training efforts are considered by DOD to be superior and we believe this is in large part responsible for the recognized successes in recent years.

Time permitting, I would like to cite two examples of recent NIS successful espionage investigations. I have included several others in the statement for the record.

One is Brian Patrick Horton, as Mr. Parker addressed. I will discuss it from the Navy viewpoint. He was an intelligence specialist second class assigned to the Fleet Intelligence Center Europe and Atlantic, Norfolk, VA.

In August 1982, information was surfaced indicating he attempted to provide top secret and special compartmented intelligence material to the Soviet Embassy, Washington, DC.

Investigation resulted in a general court-martial wherein Horton was found guilty and sentenced to dishonorable discharge, 6 years' confinement at hard labor, total forfeiture of all pay and allowances and reduction to E-1.

Procedures we developed in this case included a CI damage assessment as an element of the court-martial pretrial agreement, which has since become a model for all such investigations.

The second case was Hans Palmer Wold. He was also an intelligence specialist seaman assigned to the U.S.S. *Ranger* (CV 61), a carrier in San Diego, CA.

In July 1983, he was apprehended in Olongapo City, Republic of the Philippines [RP], for being an unauthorized absentee. During apprehension, NIS agents discovered a roll of 35-millimeter film which contained top secret/SI information which he intended to sell to the Soviet Embassy in Manila, RP.

Investigation resulted in conviction by general court-martial with a sentence of 4 years of confinement at hard labor, forfeiture of all pay and allowances, reduction to E-1, and a dishonorable discharge.

Additional examples of recent successful espionage cases are in the statement you have before you.

Despite the recent events predicating this hearing, I would like to emphasize that because of the improved posture of the Navy FCI Program, vis-a-vis 20 years ago, we are in a better position today to identify and neutralize attempts to access our classified information.

Gentlemen, thank you for your time and attention. Following the statement of Mr. Bob Allen regarding Navy security policy, I stand ready to answer any questions.

Mr. ENGLISH. Thank you.

[The prepared statement of Mr. McCullah follows:]

STATEMENT OF LANNY E. MCCULLAH
ASSISTANT DIRECTOR FOR COUNTERINTELLIGENCE
NAVAL INVESTIGATIVE SERVICE

BEFORE THE
GOVERNMENT INFORMATION, JUSTICE AND
AGRICULTURE SUBCOMMITTEE, OF THE
COMMITTEE ON GOVERNMENT OPERATIONS,
HOUSE OF REPRESENTATIVES

JUNE 17, 1985

BEST COPY AVAILABLE

MR. CHAIRMAN AND MEMBERS OF THE SUBCOMMITTEE:

I WELCOME THE OPPORTUNITY TO PRESENT AND EXPLAIN THE NAVAL INVESTIGATIVE SERVICE (NIS) FOREIGN COUNTERINTELLIGENCE (FCI) PROGRAM DESIGNED TO COMBAT ESPIONAGE IN THE NAVAL ESTABLISHMENT. I WILL ADDRESS THAT MISSION FROM THE STANDPOINT OF MANPOWER ALLOCATIONS, ORGANIZATIONAL STRUCTURE, JURISDICTION, EXAMPLES OF RECENT ESPIONAGE CASES, AN EXAMPLE OF A RECENT COUNTERESPIONAGE OPERATION AND THE PILOT FCI POLYGRAPH PROGRAM.

NIS MISSION

THE NIS MISSION COMPRISES THREE MAJOR OPERATIONAL FUNCTIONS:

CRIMINAL INVESTIGATIONS (FELONY TYPE VIOLATIONS);

COUNTERINTELLIGENCE;

PHYSICAL SECURITY/LAW ENFORCEMENT POLICY

NIS ORGANIZATIONAL STRUCTURE

THE NAVAL INVESTIGATIVE SERVICE IS CENTRALLY CONTROLLED BY ITS HEADQUARTERS IN WASHINGTON, D.C., AND FUNCTIONS OPERATIONALLY THROUGH THE FOLLOWING COMMAND STRUCTURE:

NIS HEADQUARTERS	CENTRAL CONTROL/VERTICAL STRUCTURE
REGIONAL OFFICES	10
RESIDENT AGENCIES	70
RESIDENT UNITS	65
RESIDENT UNITS AFLOAT	15
FORENSIC LABORATORIES	4

NIS SPECIAL AGENT STAFFING WORLDWIDE

THE FOLLOWING REPRESENTS THE WORLDWIDE STAFFING OF CIVILIAN SPECIAL AGENTS BY REGIONAL OFFICES AND THE HEADQUARTERS:

REGIONAL OFFICES	SPECIAL AGENTS
NEW YORK	106
MORPOLE	164
CHARLESTON	108
NEW ORLEANS	59
SAN DIEGO	144
SAN FRANCISCO	93
EUROPE	49
PACIFIC	57
JAPAN	64
PHILIPPINES	43
<u>NISHQ</u>	<u>87</u>
TOTAL	974

NIS PCI DEDICATION

PRIOR TO FY 1982, THERE WAS NO PURE DEDICATION IN THE PCI AND FRAUD ARENAS. RATHER, GENERAL SERVICE SPECIAL AGENTS WERE EXPECTED TO PERFORM SUCH ACTIVITIES IN CONJUNCTION WITH THEIR OTHER ASSIGNED DUTIES. WITH THE ADVENT OF THE DIRECTOR OF CENTRAL

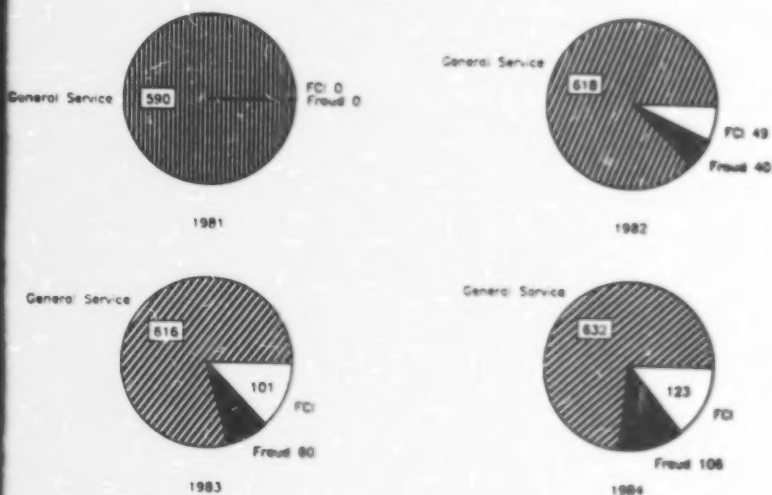
INTELLIGENCE'S OVERALL FCI PROGRAM AND THE CORRESPONDING INCREASES IN MANPOWER ALLOCATIONS, NIS SPECIAL AGENTS HAVE SINCE BEEN IDENTIFIED FOR TOTAL DEDICATION TO THE FCI PROGRAM. IN ADDITION, OUR OTHER SPECIAL AGENTS ARE ALSO EXPECTED TO PERFORM FCI ACTIVITIES, DEPENDING ON LOCATIONS AND AS NEEDED, ALONG WITH THEIR OTHER DUTIES. OUR AGENTS ALL COME ABOARD WITH AT LEAST ONE COLLEGE DEGREE, AND RECEIVE A COMBINATION OF ON THE JOB TRAINING AND ELEVEN WEEKS INTENSIVE BASIC INVESTIGATIVE TRAINING, FOLLOWED BY MORE ON THE JOB TRAINING BEFORE BECOMING ELIGIBLE FOR SELECTION TO THE FCI PROGRAM. SPECIALIZED TRAINING AS OUTLINED, INFRA, THEN BEGINS.

NIS SPECIAL AGENT ALLOWANCE

FY 1981 - 1984

THE FOLLOWING PIE CHARTS REPRESENT THE ALLOCATION OF DEDICATED GENERAL SERVICE, FCI AND FRAUD SPECIAL AGENTS IN THE NAVAL INVESTIGATIVE SERVICE DURING FY 1981 - 1984:

NIS Special Agent Allowance
FY 1981 - 1984

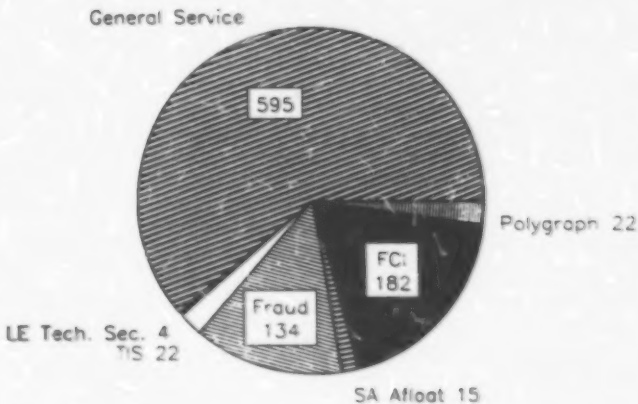


NIS SPECIAL AGENT ALLOWANCE

FY 1985

THE FOLLOWING PIE CHART BREAKS DOWN NIS CIVILIAN SPECIAL AGENTS FOR FY 1985 INTO THE DISCIPLINES OF GENERAL SERVICE, PCI, FRAUD, TECHNICAL INVESTIGATIVE SERVICES (TIS), SPECIAL AGENT AFLOAT (PRIMARYLY ON AIRCRAFT CARRIERS), POLYGRAPH AND LAW ENFORCEMENT/PHYSICAL SECURITY (LE/PS):

NIS Special Agent Allowance
FY 1985



RATIO OF NIS INVESTIGATIVE ASSETS

THE FOLLOWING REPRESENTS THE SUPPORT RATIO OF NAVAL INVESTIGATIVE SERVICE CIVILIAN SPECIAL AGENTS TO ACTIVE DUTY AND CIVILIAN EMPLOYEES WITHIN THE DEPARTMENT OF THE NAVY:

<u>SERVICE ELEMENT</u>	<u>MILITARY/CIVILIAN PERSONNEL</u>	<u>NIS SPECIAL AGENTS</u>	<u>SUPPORT RATIO</u>
NAVY/MARINE COPRS	1,084,232	974	1/1113
	NIS CI MANPOWER		

THE FOLLOWING IS A LISTING OF THE NAVAL INVESTIGATIVE SERVICE CI MANPOWER BY MAN YEARS (ALL ASSETS) COMMENCING IN FY 1981 AND PROJECTED THROUGH FY 1986:

FY 81	106 MAN YEARS	
FY 82	161 MAN YEARS	+244%
FY 83	199 MAN YEARS	
FY 84	259 MAN YEARS	+388%
FY 85	349 MAN YEARS	
FY 86	411 MAN YEARS	

GENERAL JURISDICTIONAL CONSIDERATIONS

THE RESPONSIBILITY OF THE NAVAL INVESTIGATIVE SERVICE FOR ALL COUNTERINTELLIGENCE (CI) MATTERS FOR THE DEPARTMENT OF THE NAVY (DON), LESS THOSE COMBAT-RELATED CI FUNCTIONS ASSIGNED TO MARINE CORPS COUNTERINTELLIGENCE, IS CLEARLY SPELLED OUT IN SECRETARY OF THE NAVY INSTRUCTION 5520.3, ENTITLED "CRIMINAL AND SECURITY INVESTIGATIONS AND RELATED ACTIVITIES WITHIN THE DEPARTMENT OF THE NAVY." THIS RESPONSIBILITY IS FURTHER ELABORATED IN THE 5 APRIL 1979 "AGREEMENT GOVERNING THE CONDUCT OF DEFENSE DEPARTMENT COUNTERINTELLIGENCE ACTIVITIES IN CONJUNCTION WITH THE FEDERAL BUREAU OF INVESTIGATION," SIGNED BY THE SECRETARY OF DEFENSE AND ATTORNEY GENERAL. THIS AGREEMENT PRESCRIBES THE FOLLOWING CI INVESTIGATIVE JURISDICTION FOR NIS:

A. WITHIN THE UNITED STATES, ITS TERRITORIES AND POSSESSIONS:

1. NIS HAS INVESTIGATIVE JURISDICTION OVER ACTIVE DUTY MEMBERS OF THE U. S. NAVY AND MARINE CORPS.
2. WHILE FBI HAS INVESTIGATIVE JURISDICTION OVER RETIRED MILITARY PERSONNEL, ACTIVE AND INACTIVE RESERVISTS AND NATIONAL GUARD MEMBERS, NIS WOULD HAVE JURISDICTION FOR INVESTIGATION OF ACTIONS PERPETRATED BY SUCH PERSONS WHILE THEY WERE ON ACTIVE DUTY IN THE U. S. NAVY OR MARINE CORPS.

B. ABROAD

1. NIS HAS INVESTIGATIVE JURISDICTION OVER ACTIVE DUTY MEMBERS OF THE U. S. NAVY AND MARINE CORPS, AS WELL AS OVER CURRENT CIVILIAN EMPLOYEES AND THE DEPENDENTS OF MILITARY AND CIVILIAN PERSONNEL. THE LATTER JURISDICTION OVER CIVILIANS EXISTS ONLY IN THE ABSENCE OF SUCH RESPONSIBILITY HAVING BEEN ASSIGNED OTHERWISE PURSUANT TO AGREEMENT WITH THE HOST GOVERNMENT, U. S. LAW OR EXECUTIVE DIRECTIVE.
2. INVESTIGATIONS OF RETIRED MILITARY PERSONNEL, ACTIVE AND INACTIVE RESERVISTS, NATIONAL GUARD MEMBERS, CONTRACTOR PERSONNEL, AND OTHER U.S. PERSONS, WHO PERMANENTLY RESIDE IN SUCH LOCATIONS, ARE UNDERTAKEN IN CONSULTATION WITH THE FBI, CIA, AND THE HOST GOVERNMENT AS APPROPRIATE.

C. GENERAL PROVISOS

1. NOTHING IN THIS AGREEMENT PREVENTS NIS FROM UNDERTAKING, IN A MANNER CONSISTENT WITH APPLICABLE LAW AND EXECUTIVE BRANCH POLICY, INVESTIGATIONS IN THOSE CASES WHERE THE FBI CHOOSES TO WAIVE INVESTIGATIVE JURISDICTION. THE PURPOSE FOR SUCH INVESTIGATION WOULD BE TO ESTABLISH OR REFUTE THE FACTUAL BASIS REQUIRED FOR AN AUTHORIZED

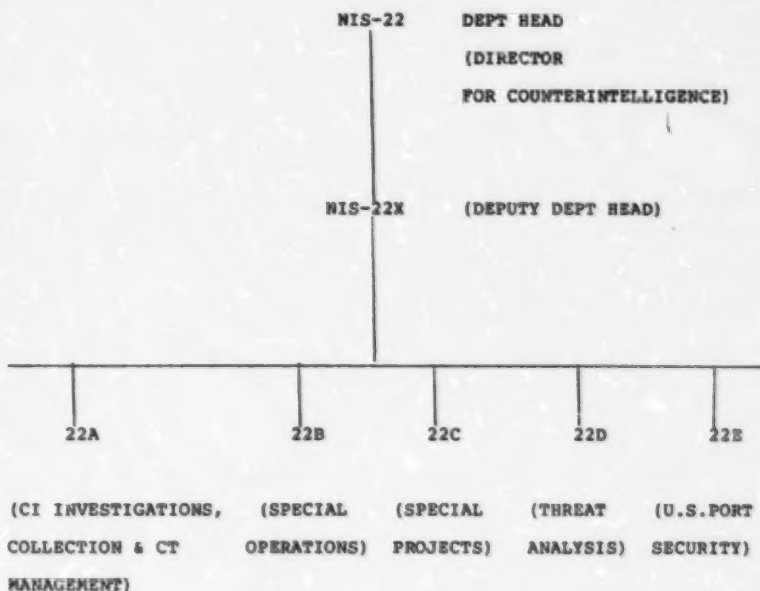
ADMINISTRATIVE ACTION TO PROTECT THE SECURITY OF DON PERSONNEL, INFORMATION, ACTIVITIES AND INSTALLATIONS.

2. THIS AGREEMENT FURTHER AUTHORIZES NIS TO PROVIDE ASSISTANCE TO THE FBI OR THE SECURITY SERVICE OF A HOST GOVERNMENT (ABROAD) IN SUPPORT OF ANY CI INVESTIGATIONS UNDER FBI JURISDICTION OR A FOREIGN GOVERNMENT (ABROAD) FOR WHICH NIS WAS NOT OTHERWISE ASSIGNED INVESTIGATIVE RESPONSIBILITY, BUT WHICH COULD IMPACT UPON THE SECURITY OF DON ELEMENTS.

NIS HEADQUARTERS INTERNAL SECURITY DEPARTMENT

THE FOLLOWING ORGANISATIONAL CHART DEPICTS THE FIVE PCI
OPERATING DIVISIONS AT NIS HEADQUARTERS:

INTERNAL SECURITY DEPARTMENT



NIS CI TRAINING

THE FORMAL NAVAL INVESTIGATIVE SERVICE CI TRAINING PROGRAM, WHICH IS CENTRALLY DIRECTED BY NIS HEADQUARTERS, CONSISTS OF TEN SEPARATE COURSES DESIGNED TO ENCOMPASS ALL ASPECTS ASSOCIATED WITH THE NIS CI MISSION. THE COURSES, WHICH RANGE IN DURATION FROM ONE TO TWO WEEKS AND REPEATED AS NECESSARY, ARE AS FOLLOWS:

- FCI COLLECTION
- SPECIAL PROTECTION & ANTI-TERRORISM
- TECHNOLOGY TRANSFER
- SPECIAL PROJECT SUPPORT
- HOSTAGE NEGOTIATION/COUNTER-TERRORISM
- COUNTERESPIONAGE/COUNTERINTELLIGENCE
- COUNTERESPIONAGE CASE OFFICERS
- COUNTERINTELLIGENCE INVESTIGATIONS
- CI ORIENTATION FOR MID-LEVEL/SENIOR MANAGERS
- OPERATIONS SECURITY (OPSEC)

ONE EXAMPLE OF OUR TRAINING CURRICULUM, AND SPECIFICALLY RELATED TO TODAY'S INQUIRY, IS OUR COUNTERINTELLIGENCE INVESTIGATIONS COURSE (CII). THE NIS CONVENES SEVERAL CII COURSES PER YEAR FOR APPROXIMATELY 30 NIS SPECIAL AGENTS PER CLASS. THIS FORTY HOUR CONCENTRATED COURSE COVERS VARIOUS AREAS OF COUNTERINTELLIGENCE INVESTIGATIONS. IT STRESSES, IN PARTICULAR,

ESPIONAGE INVESTIGATIONS AND THE FOREIGN INTELLIGENCE SURVEILLANCE ACT (FISA) OF 1978. INSTRUCTORS INCLUDE ATTORNEYS FROM THE OFFICE OF INTELLIGENCE POLICY REVIEW, DEPARTMENT OF JUSTICE, AS WELL AS PERSONNEL FROM THE FBI AND THE OFFICE OF THE NAVY JUDGE ADVOCATE GENERAL. THE PREPONDERANCE OF INSTRUCTION IS PRESENTED BY EXPERIENCED NIS FCI SPECIAL AGENTS.

FCI FUNCTIONAL AREAS

I WILL NOW ADDRESS THE SUPPORTING RELATIONSHIP THAT EXISTS BETWEEN FCI INVESTIGATIONS, COUNTERESPIONAGE OPERATIONS AND FCI COLLECTION.

NIS FCI INVESTIGATIONS

NIS FCI INVESTIGATIONS ARE BROKEN DOWN INTO THE MAJOR CATEGORIES OF:

ESPIONAGE;

LEAKAGE, LOSS, OR COMPROMISE OF CLASSIFIED MATERIAL;

TECHNOLOGY TRANSFER VIOLATIONS;

TERRORISM, AND RELATED THREAT ASSESSMENTS.

EXAMPLES OF RECENT NIS ESPIONAGE INVESTIGATIONS
THAT HAVE BEEN ADJUDICATED

AS A MATTER OF INTEREST, NIS HAS INVESTIGATED EIGHTEEN
SIGNIFICANT ESPIONAGE CASES IN THE LAST FOUR YEARS. FOR YOUR
INFORMATION TODAY, I HAVE INCLUDED THE FOLLOWING FOUR SUMMARIES:

BRIAN PATRICK HORTON

DUTY STATION: FLEET INTELLIGENCE CENTER EUROPE/ATLANTIC
NORFOLK, VIRGINIA

SUMMARY: ATTEMPTED TO PROVIDE TOP SECRET (SI) MATERIAL
TO SOVIET EMBASSY, WASHINGTON, D.C.

WHEN: AUGUST 1982

CLEARANCE LEVEL: TOP SECRET/SI

PROFILE: WHITE MALE, 28 YEARS OLD, INTELLIGENCE
SPECIALIST SECOND CLASS, MARRIED, BI-SEXUAL,
NARCOTICS USER.

COURT ACTION: GENERAL COURT-MARTIAL, GUILTY, SENTENCED TO
DISHONORABLE DISCHARGE, SIX YEARS CONFINEMENT
AT HARD LABOR, TOTAL FORFEITURE OF ALL PAY
AND ALLOWANCES AND REDUCTION TO E-1.

"HORTON CLAUSE"

BASED UPON EVIDENCE ACCUMULATED DURING THE INVESTIGATION, HORTON ELECTED TO PLEAD GUILTY UNDER A PRETRIAL AGREEMENT WHICH INCLUDED A POST-TRIAL GRANT-OF-IMMUNITY. THIS ALLOWED QUESTIONING AND POLYGRAPH OF HORTON AFTER HIS CONVICTION AND SENTENCING, FOR A PERIOD OF UP TO SIX MONTHS, TO DETERMINE ANY DAMAGE TO NATIONAL SECURITY CAUSED BY HIS ACTIONS. ALTHOUGH HORTON POSSESSED AN EXTREMELY SENSITIVE TOP SECRET CLEARANCE, THE DAMAGE TO NATIONAL SECURITY WAS DETERMINED TO BE MINIMAL. THIS TECHNIQUE, NOW LABELED THE "HORTON CLAUSE" BY THE NIS, ALLOWS NOT ONLY FOR PROSECUTION BUT FOR A DETERMINATION AS TO ANY POSSIBLE DAMAGE TO NATIONAL SECURITY. PREVIOUSLY, MANY ESPIONAGE INVESTIGATIONS WERE APPROACHED PRIMARILY FROM THE STANDPOINT OF ACQUIRING THE DAMAGE ASSESSMENT FIRST AND PROSECUTION SECOND. THE PROBLEM WITH THAT APPROACH IS THAT IT LEFT LITTLE INCENTIVE FOR THE SUSPECT TO COOPERATE WITH THE GOVERNMENT SINCE HE HAD NOTHING TO GAIN BY THIS COOPERATION. WITH THE ADVENT OF THE "HORTON CLAUSE," THE DAMAGE ASSESSMENT IS CONSIDERED DURING OR AFTER THE PROSECUTION PHASE TO ENCOURAGE THE SUSPECT THROUGH HIS COUNSEL TO COOPERATE UNDER A POST-TRIAL GRANT-OF-IMMUNITY IN AN EFFORT TO REDUCE HIS SENTENCE. THE GOVERNMENT CAN THEN INTERVIEW AND POLYGRAPH THE INDIVIDUAL AS MUCH AS NEEDED TO ENSURE HIS TRUTHFULNESS IN DISCLOSING ALL RELEVANT INFORMATION. IF THE INDIVIDUAL DOES COOPERATE AND DOES NOT DISPLAY DECEPTION, THE SENTENCE IS THEN REDUCED BY THE GENERAL COURT-MARTIAL (GCM) CONVENING AUTHORITY IN ACCORDANCE WITH THE TERMS OF THE PRE-TRIAL AGREEMENT.

THIS TECHNIQUE HAS BEEN USED ON SEVERAL OCCASIONS SINCE THE HORTON CASE, AND IT HAS PROVEN TO BE A VERY EFFECTIVE MEANS OF IDENTIFYING THE EXTENT OF DAMAGE TO NATIONAL SECURITY.

HANS PALMER WOLD

DUTY STATION: USS RANGER (CV-61), HOMEPORTED SAN DIEGO,
CALIFORNIA

SUMMARY: WOLD WAS APPREHENDED IN OLONGAPO CITY,
REPUBLIC OF THE PHILIPPINES FOR
BEING AN UNAUTHORIZED ABSENTEE. DURING
APPREHENSION, HIS AGENTS DISCOVERED A ROLL
OF 35MM FILM WHICH CONTAINED TOP SECRET/SI
INFORMATION.

WHEN: JULY 1983

CLEARANCE LEVEL: TOP SECRET/SI

PROFILE: WHITE MALE, 21 YEARS OLD, INTELLIGENCE
SPECIALIST SEAMAN, SINGLE, BI-SEXUAL,
NARCOTICS USER, IMMATURE PERSONALITY.

COURT ACTION: CONVICTED AT GENERAL COURT-MARTIAL.
SENTENCED TO FOUR YEARS CONFINEMENT AT
HARD LABOR, FORFEITURE OF ALL PAY AND
ALLOWANCES, REDUCTION TO E-1, AND A
DISHONORABLE DISCHARGE.

JOHN RAYMOND MAYNARD

DUTY STATION: CINCPACFLT, HAWAII

SUMMARY: 51 TOP SECRET/SI DOCUMENTS
WERE DISCOVERED IN MAYNARD'S PERSONAL
LOCKER AFTER HE DEPARTED HAWAII IN A
UNAUTHORIZED ABSENCE STATUS ENROUTE
TO A FOREIGN COUNTRY.

WHEN: AUGUST 1983

CLEARANCE LEVEL: TOP SECRET/SI

PROFILE: WHITE MALE, 19 YEARS OLD, SINGLE,
INTELLIGENCE SPECIALIST SEAMAN, IMMATURE
PERSONALITY.

COURT ACTION: CONVICTED AT GENERAL COURT-MARTIAL.
SENTENCED TO 10 YEARS CONFINEMENT

AT HARD LABOR; TOTAL FORFEITURE OF ALL
PAY AND ALLOWANCES; REDUCTION TO E-1;
DISHONORABLE DISCHARGE.

ROBERT ERNEST CORDREY

DUTY STATION: MARINE CORPS BASE, CAMP LEJEUNE,
NORTH CAROLINA

SUMMARY: CORDREY OFFERED TO SELL NUCLEAR,
BIOLOGICAL AND CHEMICAL (NBC) WARFARE
MATERIAL TO THE SOVIETS, CZECHOSLOVAKIANS,
POLES, EAST GERMANS AND WEST GERMANS

WHEN: APRIL 1984

CLEARANCE LEVEL: SECRET

PROFILE: WHITE MALE, 23 YEARS OLD, MARRIED, PRIVATE
FIRST CLASS, USMC, ARREST RECORD FOR
SEXUAL OFFENSES.

COURT ACTION: CONVICTED AT GENERAL COURT-MARTIAL.
SENTENCED TO FORFEITURE OF ALL PAY AND
ALLOWANCES, DISHONORABLE DISCHARGE,
CONFINEMENT AT HARD LABOR FOR 12 YEARS.

NIS FCI DEFENSIVE BRIEFING PROGRAM

**THE NIS FCI DEFENSIVE BRIEFING PROGRAM COVERS FOUR DISTINCT
AREAS AS FOLLOWS:**

- COUNTERTERRORISM
- TECHNOLOGY TRANSFER
- COUNTERESPIONAGE
- FOREIGN TRAVEL

THE FOLLOWING CHART DEPICTS THE NUMBER OF BRIEFINGS AND THE TOTAL AUDIENCE UNDER EACH PROGRAM FOR THE YEARS 1983 AND 1984:

FOREIGN TRAVEL

	NUMBER OF BRIEFINGS	AUDIENCE
1983	173	173
1984	206	206

COUNTERESPIONAGE

	NUMBER OF BRIEFINGS	AUDIENCE
1983	3,282	212,866
1984	3,546	211,211

COUNTERTERRORISM

	NUMBER OF BRIEFINGS	AUDIENCE
1983	938	59,847
1984	2,611	149,220

TECHNOLOGY TRANSFER

	NUMBER OF BRIEFINGS	AUDIENCE
1983	19	566
1984	153	4,876

NIS COUNTERESPIONAGE OPERATIONS

COUNTERESPIONAGE (CE) OPERATIONS ARE INCLUDED IN THE TERM COUNTERINTELLIGENCE AND REFERS TO ACTIONS TAKEN AGAINST HOSTILE INTELLIGENCE SERVICES TO COUNTER ESPIONAGE AND OTHER CLANDESTINE INTELLIGENCE ACTIVITIES DAMAGING TO THE NATIONAL SECURITY.

UNDER A MEMORANDUM OF UNDERSTANDING, NIS COUNTERESPIONAGE OPERATIONS ARE CONDUCTED JOINTLY WITH THE FBI WITHIN THE UNITED STATES. OUTSIDE THE UNITED STATES, IN ACCORDANCE WITH THE APPLICABLE DIRECTIVES, NIS CE OPERATIONS ARE COORDINATED WITH THE CIA.

SUMMARY OF A RECENT NIS CE OPERATION

THE FOLLOWING SUMMARIZES A RECENT NIS JOINT CE OPERATION, CONDUCTED WITH THE FBI, WHICH HAS RECEIVED COVERAGE IN THE NEWS MEDIA, INVOLVING ACTIVITIES BOTH WITHIN AND OUTSIDE THE UNITED STATES:

OPERATION SHOW DOWN

SCENARIO: NIS DOUBLE AGENT WALK-IN TO EAST GERMAN EMBASSY, WASHINGTON, D.C., OFFERING TO EXCHANGE USN MILITARY INFORMATION FOR MONEY.

DOUBLE AGENT: DEPARTMENT OF THE NAVY CIVILIAN ENGINEER EMPLOYED AT NAVAL ELECTRONIC SYSTEMS ENGINEERING CENTER, CHARLESTON, S.C.

INITIATED: 21 DECEMBER 1981

CONTACTS: 12 PERSONAL MEETINGS WITH EAST GERMAN
INTELLIGENCE OFFICERS
4 MEETINGS IN WASHINGTON, D.C.
7 MEETINGS IN MEXICO CITY
1 MEETING IN EAST BERLIN

HANDLERS: FIVE DIFFERENT EAST GERMAN INTELLIGENCE
OFFICERS MET WITH THE DOUBLE AGENT

MONEY: \$21,800 RECEIVED FROM EAST GERMANS FOR
DOCUMENTS

ARREST: ALFRED ZEHE, AN EAST GERMAN PHYSICIST,
APPREHENDED IN BOSTON, MASSACHUSETTS, ON
3 NOVEMBER 1983, WHILE ATTENDING A
PROFESSIONAL CONFERENCE.

TRIAL: CONSIDERED LANDMARK CASE AS ALL ESPIONAGE
ACTIVITY WITH ZEHE WAS CONDUCTED OUTSIDE THE
U.S. ZEHE PLEADED GUILTY TO SEVEN COUNTS OF
ESPIONAGE AND ONE COUNT OF CONSPIRACY.

SENTENCE: FOUR CONCURRENT EIGHT-YEAR PRISON TERMS,
\$5,000 FINE AND TWO YEARS PROBATION AFTER
RELEASE.

ADDENDUM: ZERE WAS ONE OF THE FOUR BLOC ESPIONAGE AGENTS
INVOLVED IN THE TRADE OF JUNE 11, 1985.

NIS COLLECTION AND PRODUCTION

THE FOLLOWING DESCRIBES AREAS THAT ARE PLACED UNDER THE NIS
COLLECTION AND PRODUCTION FUNCTION:

- ANTI-TERRORIST ALERT/FUSION CENTER
- NAVY COUNTERINTELLIGENCE DATA BASE
- MULTIDISCIPLINARY COUNTERINTELLIGENCE ANALYSIS
- FINISHED COUNTERINTELLIGENCE PRODUCTION
- COUNTERINTELLIGENCE COLLECTION AND REPORTING.

THE COLLECTION AND PRODUCTION FUNCTION OF THE NIS IS DIRECTED
TOWARDS IDENTIFYING AND COUNTERING THE HOSTILE INTELLIGENCE AND
RELATED UNCONVENTIONAL WARFARE THREAT TO THE DEPARTMENT OF THE
NAVY.

FCI POLYGRAPH DEVELOPMENTS

A RECENT ADDITION TO THE NAVY'S INTENSIFIED COUNTERINTELLIGENCE POSTURE IS THE INCREASED UTILIZATION OF THE POLYGRAPH INSTRUMENT IN AN ATTEMPT TO IDENTIFY AND RESOLVE POTENTIAL ESPIONAGE CASES BEFORE DAMAGE TO NATIONAL SECURITY CAN OCCUR. NIS IS CURRENTLY INVOLVED IN TWO DEPARTMENT OF DEFENSE COUNTERINTELLIGENCE POLYGRAPH SCREENING PROGRAMS. THE FIRST PROGRAM CONSISTS OF PROVIDING DIRECT SUPPORT TO THE NATIONAL SECURITY AGENCY (NSA) BY CONDUCTING POLYGRAPH EXAMINATIONS OF ALL NAVAL SECURITY GROUP PERSONNEL ASSIGNED TO NSA. THIS PROGRAM WILL CONTINUE INDEFINITELY.

THE SECOND PROGRAM IS A ONE YEAR DOD TEST PROGRAM WHICH AUTHORIZES NAVY TO SCREEN APPROXIMATELY 1200 PERSONNEL ON A SELECTED BASIS. POLYGRAPH QUESTIONS ASKED ARE NOT "LIFE STYLE" IN NATURE, BUT ARE DIRECTED SPECIFICALLY TO COUNTERINTELLIGENCE ISSUES. THEY ARE:

HAVE YOU EVER ENGAGED IN ESPIONAGE OR SABOTAGE AGAINST THE U. S.?

HAVE YOU EVER BEEN ASKED TO ENGAGE IN ESPIONAGE OR SABOTAGE AGAINST THE U. S.?

BEST COPY AVAILABLE

DO YOU HAVE PERSONAL KNOWLEDGE OF ANYONE ENGAGED IN ESPIONAGE OR SABOTAGE AGAINST THE U. S.?

HAVE YOU EVER GIVEN OR SOLD CLASSIFIED INFORMATION TO AN UNAUTHORIZED PERSON?

HAVE YOU FAILED TO REPORT ANY CONTACTS WITH A REPRESENTATIVE OF A HOSTILE COUNTRY?

THE USE OF THE POLYGRAPH FOR CI MATTERS IS AN EXCELLENT DETERRENT TO THOSE CONSIDERING INVOLVEMENT IN ESPIONAGE RELATED ACTIVITIES, AND PROVIDES ANOTHER MEANS OF IDENTIFYING PERSONS WHO HAVE ALREADY COMMITTED THEMSELVES TO SUCH ACTIVITY. THE INCREASED USE OF THE POLYGRAPH IS ENCOURAGED IN COMBATING ESPIONAGE AND WE ARE WORKING TOWARDS FURTHER EXPANSION OF THIS PROGRAM.

CONCLUSION

NIS HAS DEVELOPED A VIABLE PROGRAM DESIGNED TO COMBAT THE ESPIONAGE EFFORTS OF THE HOSTILE INTELLIGENCE SERVICES. WITH THE PROVISION OF RESOURCE ALLOCATIONS BEGINNING IN FY-82, NIS HAS BEEN ALLOWED TO EFFECT TOTAL DEDICATION OF NIS SPECIAL AGENTS ON A SELECTIVE, PROGRESSIVE BASIS. THE SUCCESSES OF THE PAST FEW YEARS IN COUNTERESPIONAGE INVESTIGATIONS AND OPERATIONS ARE DIRECTLY ATTRIBUTABLE TO THAT DEDICATION. WITH THE ALLOCATION OF ADDITIONAL DEDICATED FCI AGENT RESOURCES AND THE INCREASED SCOPE OF THE POLYGRAPH PROGRAM, I AM CONFIDENT FURTHER GAINS IN IDENTIFYING AND NEUTRALIZING ATTEMPTS TO ACCESS OUR CLASSIFIED INFORMATION WILL BE REALIZED.

Mr. ENGLISH. Mr. Allen.

STATEMENT OF ROBERT C. ALLEN, DIRECTOR, SECURITY POLICY, OFFICE OF CHIEF OF NAVAL OPERATIONS, U.S. NAVY

Mr. ALLEN. Mr. Chairman, I have submitted a statement for the record covering the Department of Navy security program. Rather than repeat the information you have before you in the record, I will just simply address changes the Navy is making as a result of our initial analysis of the Walker espionage case.

The Walker espionage case, insofar as our initial analysis can determine, has identified several security weaknesses that we want to follow up on. First is our granting of security clearances. Second is in our application of strict need to know for personnel to have access to classified information; third, our continuous evaluation of the trustworthiness of personnel; fourth, in our controls over unauthorized reproduction of classified material; and fifth, in our controls over unauthorized removal of classified material from our commands.

The Secretary of the Navy, in his message of June 10 directed certain immediate steps in the Navy. These include an immediate 10-percent reduction in security clearances. Commands were told that if a person's job did not require access to classified information, his security clearance should be withdrawn. They were also told that our eventual goal in the Navy was 50-percent reduction, and commands were told to report to us within 30 days on the first phase of this reduction.

We also told our commands to make sure that the personnel they assigned as security manager, top secret control officer and communications security custodians are qualified, to make sure that they are the best people, the kinds of people that can perform well in these very important and exacting duties. Additionally, we told our commands that where these people are subject to reinvestigation, they should order these reinvestigations immediately.

Additionally, we told our commands to inventory all their top secret and communications security holdings. We told them to do this in addition to their annual requirement to do this, and report any discrepancies immediately. We told them also to limit the areas in which classified material can be worked on and stored. We feel that by cutting back on the number of areas that have classified material, we will be able to do a better job of protecting those areas. We additionally told commands that lone access to top secret or special access material is strongly discouraged.

We also told commands to do better in protecting all classified material awaiting destruction and during the destruction process. We said it should be two people, and one of them should be at least a second-class petty officer, that witnessed removal of the material to the destruction site and witnessed its actual destruction.

We also told them to reduce their classified holdings. We told commands to look at what classified documents they have, to determine if those documents are necessary to their mission, and in the numbers of copies that they hold, and either return or destroy all unnecessary classified material.

BEST COPY AVAILABLE

We also told them to carefully review their program for continuous evaluation of eligibility for access and to ensure that all people in the command are aware of the requirement to report information bearing on trustworthiness, loyalty, reliability, and judgment to command senior personnel.

And we asked commands to beef up their random inspection of papers and articles carried by personnel entering and leaving Navy commands.

These are immediate actions. Additionally, we established a security task force of which I am the chairman, to identify longer term actions and to report to the Director of Naval Intelligence, for him to report to the Secretary of Navy, by July 12. These include other improvements to our personnel security control procedures. We are certainly looking at further ways to help commands in meeting our 50-percent reduction goal. We are looking at other innovative means of determining trustworthiness of personnel. We are looking for personnel research and development areas which the Navy can support, and we are looking at obtaining authority for increased use of the counterintelligence scope polygraph.

We also will be looking at other improvements to document control procedures. We will be looking at one area that you have already mentioned, are our commands faithfully following the classification guidance that we provide and only classifying where that is required. And, are commands very carefully limiting the number of copies of documents they make?

We will be working with our originators of classified documents to make sure the distribution lists are held to the minimum, that they only send copies of classified documents, and classified messages to those commands whose missions require that information. And we have begun to prepare for centralized adjudication of all Department of the Navy security clearances.

We expect our centralized adjudication to be in effect by October 1, 1985.

Thank you, Mr. Chairman.

Mr. ENGLISH. Thank you very much, Mr. Allen.

[The prepared statement of Mr. Allen follows:]

STATEMENT OF
ROBERT C. ALLEN
DIRECTOR, SECURITY POLICY
OFFICE OF THE
CHIEF OF NAVAL OPERATIONS
BEFORE THE
HOUSE GOVERNMENT OPERATIONS
SUBCOMMITTEE ON
GOVERNMENT INFORMATION, JUSTICE AND AGRICULTURE
ON
DEPARTMENT OF THE NAVY SECURITY PROGRAM

BEST COPY AVAILABLE

I am Robert C. Allen, Director of Security Policy, Office of the Chief of Naval Operations. I welcome the opportunity to appear before you this afternoon to discuss Navy's program for controlling access to classified information.

The basic principle governing our security program is control of access. Control is exercised by allowing access only by personnel who have been determined to be trustworthy and by imposing administrative measures to safeguard classified material from disclosure to unauthorized persons.

Navy security policies and procedures to control access are described in detail in the Department of the Navy Information and Personnel Security Program Regulation (OPNAV Instruction 5510.1G). This regulation is issued to every activity in the Navy and Marine Corps and is applicable to all military and civilian personnel in the Department.

The regulation incorporates the policies of the Department of Defense Information Security Program (DOD 5200.1-K) and the DOD Personnel Security Program (DOD 5200.2-K).

This statement for the record highlights the specific rules which govern access to classified information and controls for classified material. As the investigation of the Walker espionage case continues, we are assessing our security posture. We have embarked on initiatives to reinforce the policies and procedures in place and to implement more stringent measures where necessary.

SECURITY PROGRAM MANAGEMENT

Responsibilities for the security program are clearly defined in our regulation, with specific assignments for program management at the command level. Every command eligible to receive classified information must designate an officer or civilian (GS-11 or above) to support the commanding officer in his responsibility for effective management of the program. The security manager is the principal advisor on information and personnel security and administers the command program. Among the duties assigned, the security manager:

1. Ensures those who are to handle classified information are appropriately cleared.
2. Ensures access to classified information is limited to persons with a need to know.
3. Coordinates the command program for continuing evaluation of eligibility for access.
4. Ensures compliance with accounting and control requirements for classified material.
5. Formulates and coordinates the command security education program so all personnel are aware that classified information requires protection against unauthorized disclosure; only those who have been officially and specifically authorized may have access to classified information; any contact in any form with any citizen of a

BEST COPY AVAILABLE

communist controlled or hostile country must be reported; and any attempt by an unauthorized person to acquire classified information must be reported.

If a command handles Top Secret information, the commanding officer must designate a Top Secret Control Officer (TSCO). The minimum grade allowed is chief petty officer or senior non-commissioned officer (E-7) or civilian (GS-7). The TSCO maintains accountability for Top Secret information, keeping dissemination to the absolute minimum necessary for proper planning or action. He or she maintains a current roster of persons in the command who are authorized access to Top Secret, transmits the material within the command by direct personal contact, and maintains a continuous chain of receipts and disclosure records for all Top Secret material.

WHO MAY HAVE ACCESS

The objective of our program is to permit knowledge or possession of classified information only when official duties require access and to ensure, to the maximum extent possible, that individuals given access are trustworthy. No one may be allowed access unless a favorable determination has been made of his or her loyalty, reliability, judgment and trustworthiness. The determination of eligibility for access (clearance) is based on an investigation appropriate to the level of access required. If access to Confidential or Secret information is required, a National Agency Check by Defense Investigative Service (DIS) or a National Agency Check with Inquiry by the Office of Personnel Management is conducted. If access up to the Top Secret level is required, a more in-depth Background Investigation by DIS is conducted. The results of the investigation, as well as any other available information in respect to the person's behavior, character and personal circumstances, are reviewed in light of the security

criteria and adjudication guidelines established by the Secretary of Defense and implemented in the Navy by our security regulation. If it is proposed to deny an individual security clearance, he or she is given an opportunity to appeal a denial decision.

Policy currently requires reinvestigation by DIS every 5 years for those with access to Top Secret information. Reinvestigations are controlled by a monthly quota adjusted as resources are available at DIS. Because of the heavy caseload at DIS, our quota cannot accommodate the 5-year reinvestigation requirement and we have had to limit periodic reinvestigations to those with access to sensitive compartmented information (SCI), Top Secret Control Officers and Top Secret Communications Security Material (COMSEC) Custodians.

Under our current system, the clearance determination for civilian employees is made at a central adjudication facility in the Naval Civilian Personnel Command. For military personnel, the adjudication authority has been vested in the commanding officer. The Secretary of the Navy recently determined, however, that adjudication for all security clearances will be centralized. We are proceeding with plans to reach that goal in the near future.

The ultimate authority for granting access to classified information rests with the commanding officer who is responsible for the security of information or material in his or her command. The level of access allowed is recorded in the command.

The requirement to ensure the propriety of each individual's clearance and access is continuing and is as important as the original determination. Accordingly, our regulation requires each commanding officer to maintain a program for continuous evaluation of the propriety of an individual's clearance and access to classified information, with internal channels for reporting information bearing on a cleared individual's trustworthiness. When derogatory or questionable information is

acquired, eligibility for access must be reevaluated. If appropriate, the commanding officer may suspend or restrict access until the issue is resolved. If the individual no longer meets the security criteria, the clearance will be revoked.

The quantity and quality of information available for evaluating personnel are the key to an effective program. Personnel security specialists and behavioral scientists agree there is a real need for personnel security research to identify indicators of security significance and to develop investigative procedures and techniques to acquire the information which will reveal those security indicators. The Walker case points up the need for research to improve our capability to identify security risks which would not be discerned under our present screening and investigative process.

Psychological evaluations more clearly establishing an individual's motivations and emotional stability, as well as providing a better understanding of the significance of particular behavior, when combined with the results of investigation, would greatly enhance our security clearance process. Unfortunately, we do not presently have the resources to incorporate psychological evaluations routinely into the security clearance determination process, but may only use such evaluations in those cases when necessary to resolve issues of mental or emotional instability. Efforts are underway in the Department of Defense to identify psychological testing methodologies which could be of use in lieu of time-consuming, expensive psychological interviews and yet still provide some basis for evaluating the psychological and emotional state of the candidate for clearance. Further refinements of the investigative and adjudicative process would give us better protection against the rare exceptions who would violate the trust we place in them.

HOW CLASSIFIED INFORMATION IS SAFEGUARDED

Administrative measures are imposed to protect classified information from disclosure to unauthorized persons. Accounting and control procedures prescribe use, reproduction, storage, transmission and disposition of classified material.

Classified material is afforded a level of accounting and control commensurate with its assigned classification, with the most stringent controls placed on Top Secret information. Commanding officers are enjoined to keep their classified holdings to the minimum necessary and to destroy classified material as soon as it is no longer required so they may better protect the material they must hold.

Classified material may be used only where there are facilities or under conditions adequate to prevent unauthorized persons from gaining access by sight, sound or other means. It must be stored in approved security equipment when it is not in use or under direct supervision of authorized persons. And the commanding officer's approval is required before classified material may be removed from the designated areas of the command. Random security inspections may be conducted of articles or papers carried by persons entering or exiting Navy ships, offices or buildings which are repositories of classified information.

The means by which classified material may be transmitted from one location to another are specified, with strict controls on handcarrying classified material while in a travel status. When classified material is no longer required, it is destroyed by a method which will prevent later recognition or reconstruction. Authorized methods are burning, shredding, pulverizing, disintegrating or wet pulping. All protective measures for the level of classification must be applied to the material until destruction is completed. Two officials, cleared to the level of the material being destroyed, must witness the destruction.

BEST COPY AVAILABLE

If there is a break in security control and classified information is subjected to compromise, the security violation must be reported and vigorously investigated, the cause of the violation corrected and disciplinary action taken if appropriate. Possible acts of sabotage, espionage, deliberate compromise or other subversive activities must be reported immediately to the Naval Investigative Service.

Our security program is comprehensive and, for the most part, works well. Administrative and physical security measures designed to protect the classified information of the Navy and the government are vulnerable when a person in whom we have resided trust is determined to do harm. As a result of the Walker case, we are taking a close look at all of our procedures to apply lessons learned and to improve, in a balanced manner, our capability to protect our nation's classified information.

Mr. ENGLISH. Mr. McCullah, I want to see if you can provide any insight to my question that I asked of the FBI a little earlier.

The thing I think the American people find so disturbing about the Walker case, and we are not presuming their guilt, but simply in discussion, would be the fact that they were able to operate for 20 years without being caught. That is a very disturbing fact, and there were other people involved as well.

I have heard that there may have been a tip as much as 10 or 15 years ago that was not followed up. Can you give us any insight as to how that was able to take place, why a tip that may have been given 15 years ago apparently was not followed up?

Mr. McCULLAH. Sir, No. 1, I am not aware that that is true; and No. 2, following the guidelines that were agreed upon, I would prefer not to comment directly on the Walker case.

I will state that it is possible for someone, once they make the initial contact, by following their own good security procedures, can meet outside the United States in foreign countries that makes it very difficult for U.S. counterintelligence to pick up on.

Mr. ENGLISH. Because, as I understand it—and again, not to get into the specific circumstances—but as I understand it, most of the information that I have read about, at least in public, indicates that that was not the case. It was not information that was passed in some foreign country but was passed here in the United States.

Let me put the question to you this way. We will get a little further away from the Walker situation.

Would it alarm you that an agent, and perhaps several agents, were able to operate for as much as 20 years in this country without being discovered?

Mr. McCULLAH. Yes, sir, I would be lying if I said it did not alarm me; as a citizen and as a special agent, it alarms me.

Mr. ENGLISH. Well, the fact there is a spy is one thing. The fact that he could be there for 20 years without being discovered is what to me is extremely alarming.

You see what I am getting at, as far as the degree of concern, it seems to me it is one thing for a fellow to be a spy and to be discov-

ered as a spy, but to go for 20 years, that is what is particularly alarming. Is that correct, in your opinion? Is that a concern?

Mr. McCULLAH. I would hesitate to use the 20-year figure in reference to the Walker case.

Mr. ENGLISH. Well, let's not use it in relation to the Walker case. Let's use it—an agent. If he were able to do that for 20 years, would that be particularly alarming?

Mr. McCULLAH. I would have to say yes.

Mr. ENGLISH. Secretary Weinberger and Navy Secretary Lehman have announced their intention to reduce the number of security clearances, and, Mr. Allen, this is probably a question that is better suited for you.

Can you tell us what the plan is? Are they talking about reducing all security clearances in direct proportion, or are they just talking about doing it in one particular type of clearance? What is the plan with regard to the reduction of those clearances?

Mr. ALLEN. I believe the Secretary of Defense's statement calls for a 10-percent reduction in each area of top secret, secret and confidential. We are certainly going to try to do that within our own program and, since we are shooting for a higher goal, we hope we will have more.

Mr. ENGLISH. Secretary Lehman is shooting for 50 percent. Have you got any idea how he plans to bring that about?

Mr. ALLEN. A lot of the effort will be reducing the amount of classified material held by commands and doing what we can to reduce the amount of material that is classified.

We are the aggrieved party, the Navy. We are outraged. We are taking very aggressive action.

Mr. ENGLISH. In your statement, you came up with a lot of proposals of things that the Navy plans to do. How many of those are things that are new, brand new, as opposed to general policies that the Navy has had in the past?

Mr. ALLEN. I think, of course, the cutback in clearances is new. We did this perhaps once before that I know about; during the Ellsberg time, we cut back on top secret level clearances. But this is a more far reaching cutback.

Certainly our program for discouraging lone access to top secret and other sensitive material is something new that we have never tried before.

Our program for more inspections of people leaving and entering commands—there has always been a possibility of doing that, but we have never tried to do it to the degree that we will be doing it now.

And I think looking for better people to fill our security billets is an entirely new idea. So often in the past, junior people, people who perhaps didn't have any other place to fit, were given security jobs, and we are now trying to put the best Navy people in those jobs.

Mr. ENGLISH. Mr. McCullah, do you have the resources to adequately do the job in dealing with espionage in the Navy?

Mr. McCULLAH. No, sir. As I indicated in my statement, we have programmed for the outyears where we feel we need up to 600 at least to do additional in the FCI arena.

Mr. ENGLISH. And how many do you have now, or is that classified?

Mr. McCULLAH. I would rather not use an exact figure.

Mr. ENGLISH. We will get into that whenever we get into closed hearing and discuss that a little bit more. But you do feel that you need additional resources to adequately do your job?

Mr. McCULLAH. Yes, sir.

Mr. ENGLISH. Mr. Lightfoot, do you have some questions?

Mr. LIGHTFOOT. Thank you, Mr. Chairman.

Mr. Allen, I direct this question to you and will read one paragraph out of the letter which was sent out by Rear Admiral Carlson, as far as some of the things that are happening within the Navy to tighten up security, and you alluded to this a moment ago.

One of the things that he mentioned was reducing classified holdings, disposing of unnecessary classified materials directed by existing instructions, commands will take themselves off distribution lists for unneeded classified documents, review the command program for continuous evaluation of eligibility for access, and re-emphasize to all hands requirements for reporting information basing on loyalty, reliability, judgment and trustworthiness. Compliance with these procedures might have denied Soviet access to classified information.

I realize, as you mentioned a moment ago, that the Navy feels like it has got a bit whipped upon on this thing. On the other side of the coin, are we having possibly a knee-jerk reaction? Are we going a little bit too far, maybe? How do you feel? Where are we?

Mr. ALLEN. I think that is a good point. I think our approach has been described by the Secretary of the Navy and the Chief of Naval Operations as a balanced approach. We see that at this time, based on what has happened, there is room for improvement.

We thought we had a good program. We see now there is room for improvement. We will not overreact, but nevertheless we are making some changes.

Mr. LIGHTFOOT. Thank you.

That was the only question, Mr. Chairman.

Mr. ENGLISH. Mr. Neal.

Mr. NEAL. Just looking over your testimony, I am struck with several things. For instance, in the examples of some cases, I am curious. First of all, the examples that you used here of Wold and Horton and Maynard and Cordrey, are they there because they are fairly typical?

Mr. McCULLAH. They were recent court-martial convictions, sir, is the reason I use them as examples.

Mr. NEAL. One thing that strikes me about it is here one was a 19-year-old with top secret clearance. Another is 21 years old, top secret clearance. The other is a little older, I guess.

Did all of these offer to sell to the Soviet Union?

Mr. McCULLAH. Yes, sir.

Mr. NEAL. In other words, they weren't recruited by the Soviets?

Mr. McCULLAH. No, sir.

Mr. NEAL. These are people that just voluntarily—

Mr. McCULLAH. All of our convictions in the past 3 years, investigations and convictions, have involved people making the initial approach and offering to sell to the Soviets.

Mr. NEAL. And you were able to apprehend them by keeping an eye on those people to whom they might sell as opposed to knowing—

Mr. McCULLAH. I would rather not discuss the exact technique. They were all detected prior to the act of espionage taking place and they were all charged and convicted of attempted espionage.

Mr. NEAL. Had they made contacts with foreign agents?

Mr. McCULLAH. Yes, sir, they had made contacts, but the act had not taken place. They were stopped before the act had taken place.

Mr. NEAL. I myself am surprised, I guess, by the pattern that seems to be emerging from today's hearings, which is that in almost all of these cases we have heard about, American citizens have volunteered of their own free volition, for one reason or another, to sell valuable classified information.

Would you say that is the most common occurrence in your experience?

Mr. McCULLAH. The trend of the last few years is as you stated.

Mr. NEAL. In your opinion, have you developed a profile that might recognize some of these individuals in advance?

Mr. McCULLAH. I would hesitate to give it the dignity of an official title of profile, due to the limited number of cases and population that we studied. Yes, sir, we did go back for 15 years and study espionage investigations, and determined certain common character indicators in the majority of the cases.

I would rather not discuss those indicators in the open hearing, if I may.

Mr. NEAL. We will get into that, Mr. Chairman, won't we?

Mr. ENGLISH. Yes, indeed.

Mr. NEAL. Let me pursue one other line of questioning if I can for just a minute.

I notice that you place a good deal of reliance on the polygraph—at least in part of your testimony you suggest that you do.

Mr. McCULLAH. Yes, sir.

Mr. NEAL. Were you in the room when I said something earlier about the testimony that we had at another Government Operations Subcommittee?

Mr. McCULLAH. Yes, sir.

Mr. NEAL. How would you characterize that?

Mr. McCULLAH. I am not familiar with the gentleman that gave that testimony. I will simply have to state that it has been my personal experience and our agency's experience, as Mr. Parker indicated, that the polygraph is a very valuable tool, and I emphasize the word "tool." It is not the beginning, it is not the end. It is a tool.

Mr. NEAL. Then you consider it to be reliable, though?

Mr. McCULLAH. It has been our experience, yes, sir. I can't give you a percentage factor, but I personally consider it a reliable tool.

Mr. NEAL. And that would be based on independent verification from some other source of whatever it is you find out?

Mr. McCULLAH. Again, I am not a polygraph expert, and I can't speak to statistics. I would have to say that the utilization by our organization, with the results corroborated by separate investigation, has shown the polygraph to be reliable, yes, sir.

Mr. NEAL. I tell you I found that testimony surprising, because it had been my impression that it was reliable and so on, too.

I have been sort of haunted by it ever since I heard it. I am not expert, so I can't say whether it is accurate or not—but the problem is really twofold. One is that you would miss a lot of people who were skillful in successfully overcoming the polygraph technique, and the other, those people who would successfully pass, who might be lying, the danger being that one would place false confidence in this tool, and have in positions of trust those who are in fact lying.

Mr. McCULLAH. I don't think, sir, we should place total reliance in it and/or it should be the sole tool. I think it would assist in identifying possible suspect. I would also venture to say; if any of those individuals charged would have perhaps been subjected to polygraph during the course of their career, I very seriously doubt it would have lasted the 20 years that Chairman English is concerned about.

Mr. NEAL. Is that right?

Mr. McCULLAH. It is my personal opinion, sir.

Mr. NEAL. Is it unusual for a 19-year-old to have a top security clearance?

Mr. ALLEN. No, sir.

Mr. NEAL. It is not unusual?

Mr. ALLEN. No. The services—I am sure it is true of all the services—the Navy is a very young group of people. Most of our people are very young. These people come into the Navy and they go through their schooling and are immediately assigned to duties in which they are required to have that type of access.

Mr. NEAL. I have an 18-year-old son. I went through the experience of him—

Mr. ALLEN. I think a very significant point.

Mr. NEAL [continuing]. Totaling a car last night. And I find him to be a very honest individual. But I may be extrapolating from that experience. I am not sure however, that top secret information should be entrusted to all the 18- and 19-year-olds I know. I am sorry.

Mr. ALLEN. I was going to make a point. We don't really get much in the investigation to tell us about that individual—he is a very young person; he hasn't dealt with many things in life. The investigations on young people are limited in what they can tell us so that makes it very difficult to make clearance determination.

Mr. NEAL. Thank you.

Mr. ENGLISH. Thank you very much.

That, then, underscores the need for reinvestigation with young people like that. They are developing their character—I should say, developing further. And it is, I would think, a time in which they are very volatile; many young people are.

Mr. ALLEN. That is true, Mr. Chairman.

Mr. ENGLISH. So instead of having the investigation, reinvestigation once every 5 years, if it goes to the 17-year-old, it appears now, that is a damaging situation indeed.

Mr. ALLEN. Yes. We feel very strongly that a periodic reinvestigation is very important. Because after they have been in the Navy for a few years and had to learn how to handle money and deal

with new friends and deal with the pressures of having classified material, a reinvestigation can provide more meaningful information on a person's trustworthiness.

Also, on the polygraph issue I would like to say we see it as a very important deterrent. It is a useful tool. And, if we had that deterrent in front of people—that they, as a person who has access to sensitive classified material, may be polygraphed using counter-intelligence polygraph questions, I think some of them who find it so easy to accept money for espionage would have second thoughts.

Mr. ENGLISH. OK.

I want to thank you both. We will have written questions for you, and we will be talking to you later when we have a closed hearing. We will get into some of these details a good deal deeper than we are here.

I would like to make a closing statement. We began these hearings with the hope of shedding some light on the problems of our intelligence programs, the classification system, and the security clearance process. I recognize that we cannot expect to draw any final conclusions from the sensitive subjects based solely on the information available at the public hearing. Nevertheless, there has been one persistent theme, and that is the lack of resources.

GAO identified a number of areas in which work needs to be done. The FBI told us that they need more resources to maintain proper controls over Soviet agents in this country. DOD has also indicated that they need more resources to oversee the classification system.

It may be that some of the problems that have come to light recently are the result of persistent failure to devote enough attention to the basic elements of our own security system. The controls have eroded and the results of these failures are recorded in dramatic headlines on the evening news. Some efforts to address these problems have already been announced.

The subcommittee will continue its investigation in order to make sure that all of the problems are identified and that the appropriate solutions are found and implemented.

I want to thank all of our participants in today's hearings for their cooperation.

Any other members of the subcommittee have any comments they would like to make?

OK, with that we will recess subject to the call of the Chair. Thank you again.

[Whereupon, at 4:35 p.m., the subcommittee adjourned, to reconvene subject to the call of the Chair.]

